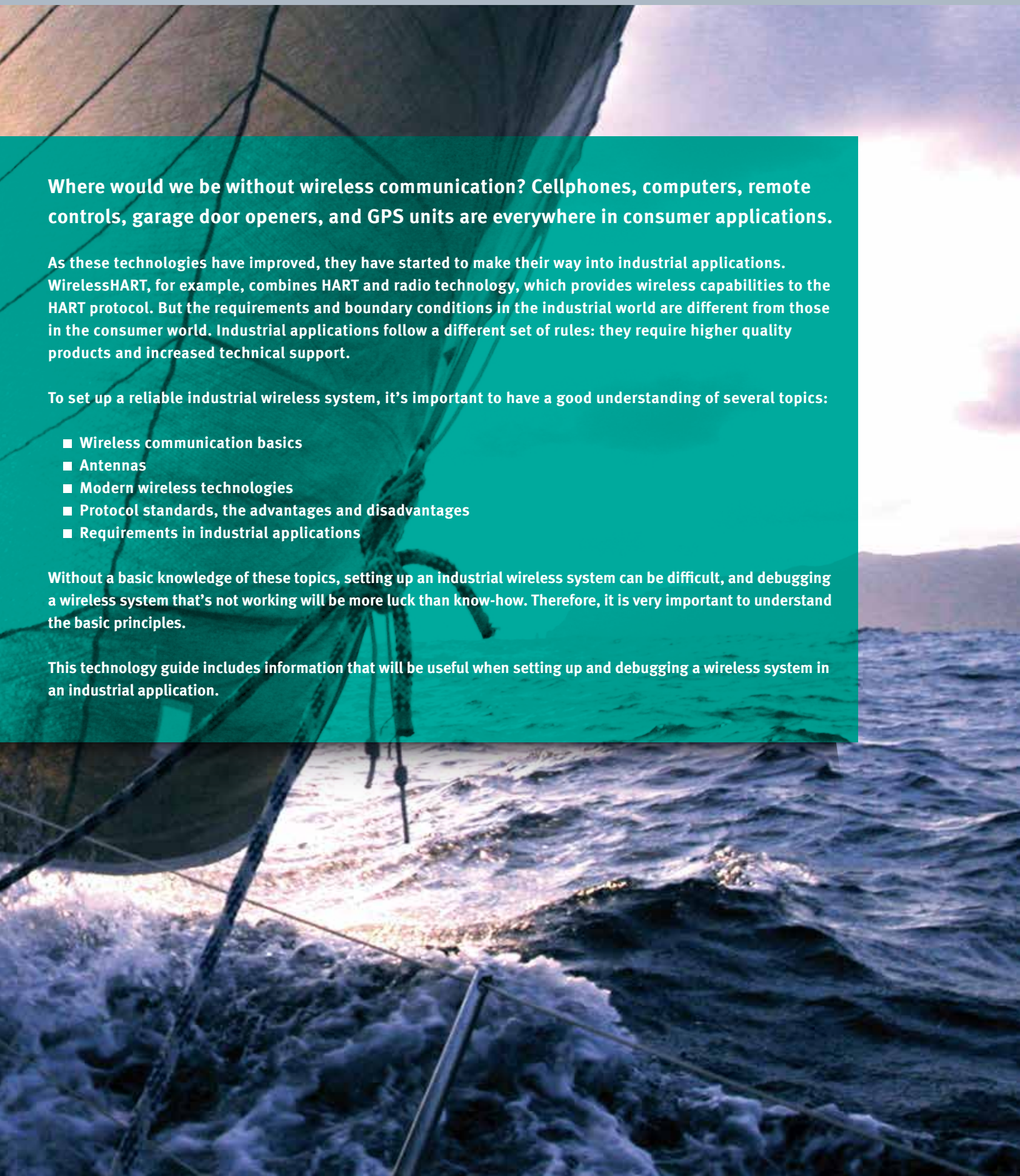
WIRELESS TECHNOLOGY

TECHNOLOGY GUIDE

PEPPERL+FUCHS
PROTECTING YOUR PROCESS



Where would we be without wireless communication? Cellphones, computers, remote controls, garage door openers, and GPS units are everywhere in consumer applications.

As these technologies have improved, they have started to make their way into industrial applications. WirelessHART, for example, combines HART and radio technology, which provides wireless capabilities to the HART protocol. But the requirements and boundary conditions in the industrial world are different from those in the consumer world. Industrial applications follow a different set of rules: they require higher quality products and increased technical support.

To set up a reliable industrial wireless system, it's important to have a good understanding of several topics:

- Wireless communication basics
- Antennas
- Modern wireless technologies
- Protocol standards, the advantages and disadvantages
- Requirements in industrial applications

Without a basic knowledge of these topics, setting up an industrial wireless system can be difficult, and debugging a wireless system that's not working will be more luck than know-how. Therefore, it is very important to understand the basic principles.

This technology guide includes information that will be useful when setting up and debugging a wireless system in an industrial application.

CONTENTS

1 THE BASICS

1.1 Electromagnetic spectrum **4**

1.2 Propagation of waves **5**

1.2.1 Free Space Propagation 6

1.2.2 Real Propagation 6

1.2.3 Reasons for Shorter Distance in Real Environment 8

1.2.4 Changing Environment 12

1.2.5 Conclusion 12

2 TECHNICAL PREREQUISITES

2.1 Modulation **13**

2.1.1 FHSS 14

2.1.2 DSSS 14

2.1.3 Consequences of Better Modulation Techniques 16

2.1.4 Conclusion 16

2.2 Antennas **17**

2.2.1 Antenna Characteristics 18

2.2.2 Antenna Gain 19

2.2.3 Conclusion 19

2.3 Energy Supply **20**

2.3.1 Mains Powered 20

2.3.2 Energy Harvesting 20

2.3.3 Galvanic Cells 21

2.3.4 Conclusion 22

2.4 Encryption **23**

2.4.1 WEP and WPA 24

2.4.2 WPA2/AES 24

2.4.3 Special Operating Modes of Encryption 25

2.4.4 Conclusion 26

3 REGULATIONS AND STANDARDS

3.1 ISM Bands **27**

3.1.1 800 – 900 MHz 27

3.1.2 2.4 GHz 28

3.2 Worldwide Standards **28**

3.2.1 IEEE 802.11 (WLAN) 28

3.2.2 IEEE 802.15.1 (WPAN / Bluetooth) 29

3.2.3 IEEE 802.15.4 (Low Rate WPAN / ZigBee) 30

3.2.4 Comparison 31

3.2.5 Coexistance 32

3.2.6 Conclusion 33

3.3 Network Topologies **34**

3.3.1 Star 34

3.3.2 Mesh 35

3.3.3 Star Mesh 36

3.3.4 Conclusion 37

4 INDUSTRIAL WIRELESS COMMUNICATION

4.1 General Conditions for Using Wireless Technology **38**

4.2 Classes of Industrial Applications **39**

4.3 Special Conditions for Using Wireless Technology **40**

4.3.1 Factory Automation 40

4.3.2 Process Automation 40

4.3.3 Conclusion 41

5 TABLES, FIGURES, AND SOURCES

Tables **41**

Figures **41**

Sources **42**

1.1 ELECTROMAGNETIC SPECTRUM

Radio waves are, as light, part of the electromagnetic spectrum which describes different types of electromagnetic waves. The only difference between light and radio waves is the wavelength or the frequency with which the waves oscillate. Different descriptions are used for the different frequencies, such as UHF, microwave, infrared, ultraviolet, etc.

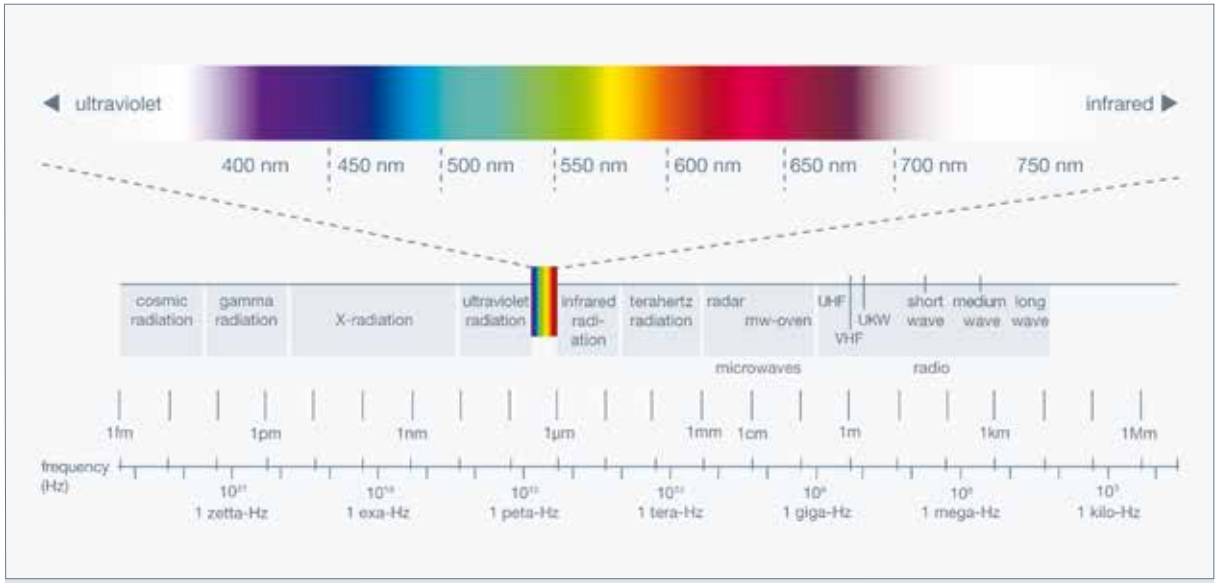


Figure 1: Electromagnetic spectrum

Radio waves range in frequency from 10 kHz to 100 GHz, which is further divided into bands (see 2.1).

Another aspect of light that also applies to the invisible part of the electromagnetic spectrum is the frequency dependency. The frequency dependency, which will be discussed later, has different electromagnetic effects, one of which can be demonstrated with light refraction through a prism.

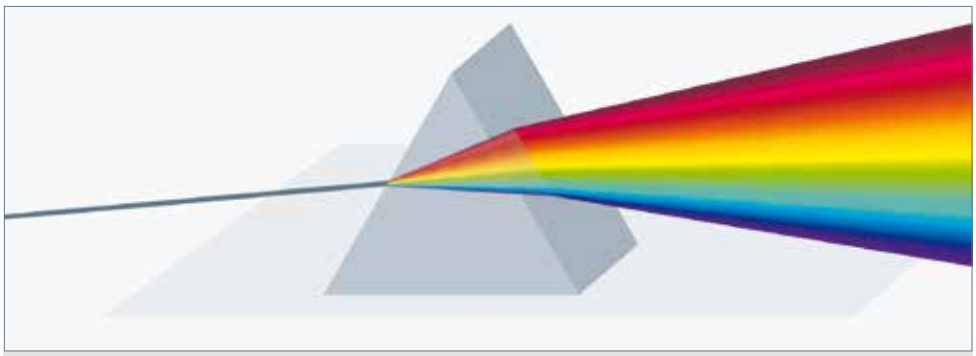


Figure 2: Light refraction on a prism

1.2 PROPAGATION OF WAVES

An important property of radio waves is spherical propagation from the source (antenna), single radio waves propagate equally in all directions. This is comparable to a light bulb, which does not project light in just one, but in (almost) all directions.

Spherical propagation has an important consequence: The radiation density decreases with increasing distance from the source. The correlation of the distance to the radiation density is shown in the graphic below:

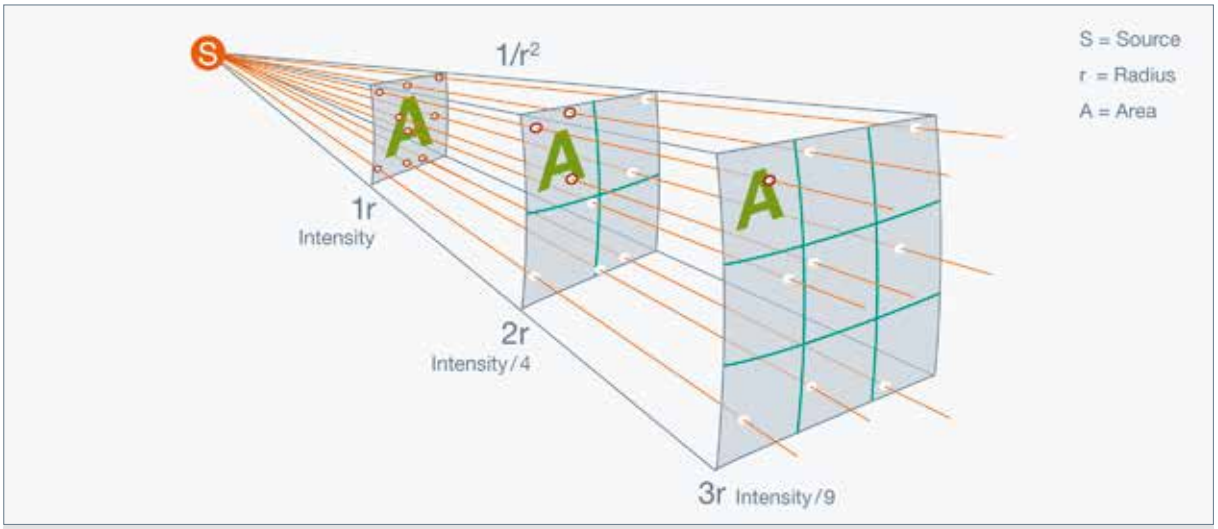


Figure 3: Inverse square law

The result is that, with increasing distance, the density of the signal decreases with the function $1/r^2$. When doubling the distance, the signal density is just ¼, with tripling the distance the signal density is ⅑.

Decibel

The attenuation of a signal is usually described in decibels (dB). A decibel is a logarithmic calculation tool that puts two numbers in relationship to each other.

dB	Factor
-20	0.01
-10	0.1
-6	0.5
0	1
6	2
10	10
20	100

Decibel alone has no meaning, the physical value to which it is compared must be added. For example, dBm means that the compared value is mW, dBW relates to Watt, dBV to V. Calculating with decibels makes it easy to calculate amplifications and attenuations since multiplications are transformed into simple additions and substractions. Also, the numbers do not become so big or small when multiplying or dividing multiple times.

For example, if a sender transmits with 8 dBm with an antenna that has antenna gain of 2 dB and the path has losses of 85 dB, the receiver receives -75 dBm. A loss of 10 dBm means that the output power is 1/10 of the original input power and a loss of 20 dBm is 1/100 of the original input power. Alternatively, a gain of 10 dBm is 10 times the original input power and 20 dBm is 100 times the original input power.

1.2.1 FREE SPACE PROPAGATION

When radio waves propagate freely in all directions and without obstacles, it is described as a free space propagation. The loss in relation to the distance from the sender can be shown as follows:

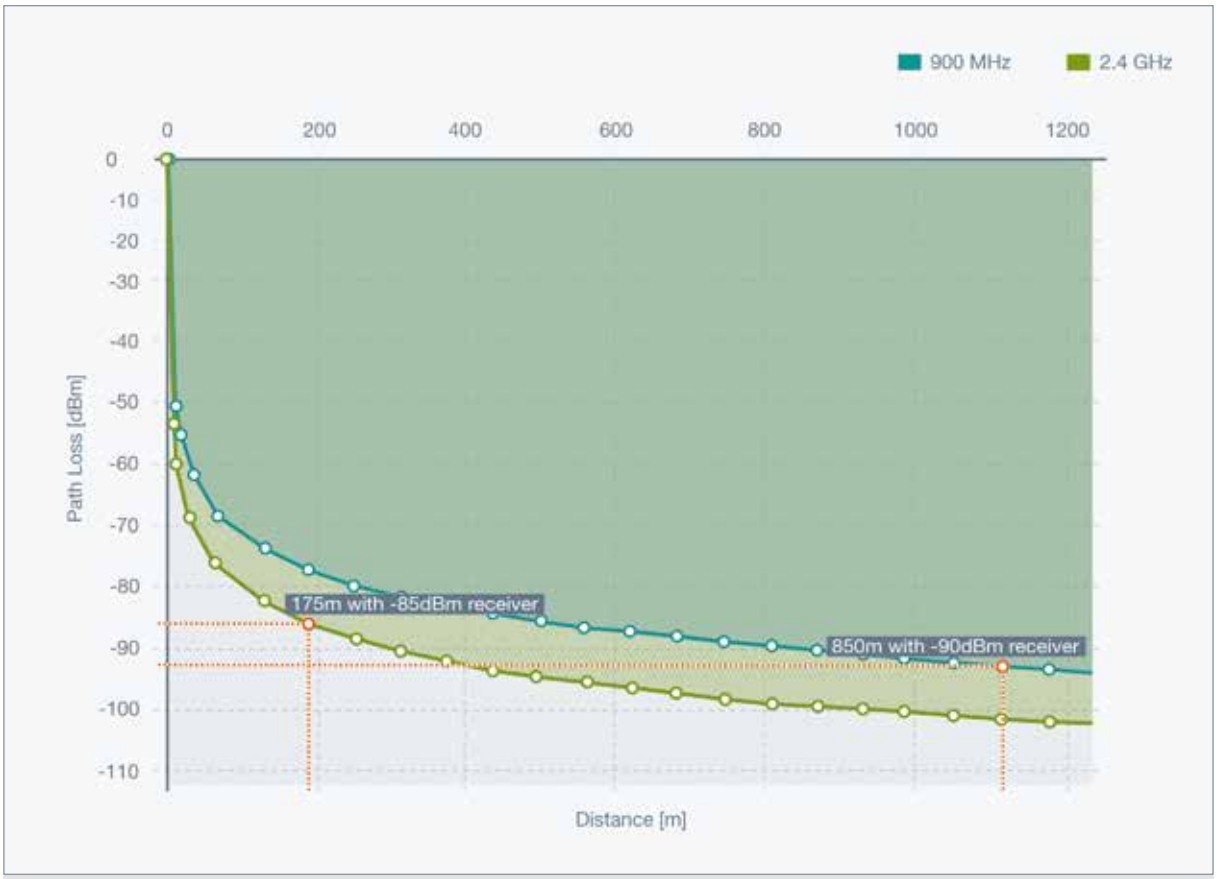


Figure 4: Theoretical free space propagation

Here, free space is considered with the atmosphere including rain, fog, snow, dust, and smog. For local networks, these effects show no relevant negative influence. For example, 2.4 GHz signals may be attenuated by up to 0.0 dB/km by torrential rain (4 inches/hr or 100 mm/hr or 100 l/m2 per hour). Thick fog produces up to 0.02 dB/km (0.03 dB/mile) attenuation. For local networks, these effects can be neglected. They are only important for cell phone or satellite communication; therefore, they are not covered in this brochure.

1.2.2 REAL PROPAGATION

This is a theoretical picture that illustrates how much a wave is damped. In reality, the environment must be taken into account. For this, several damping factors are empirically evaluated:

The table shows that the path loss is larger as more structures and materials are included in the environment. The path loss exponent increases the damping of the signal significantly.

Environment	Path Loss Exponent
Free space	2
Urban environment	2.7 to 3.5
Shadowed urban environment	3 to 5
Inside of buildings with no line of sight	4 to 6
Inside of factories with no line of sight	2 to 3

Table 1: Path loss exponent for different environments

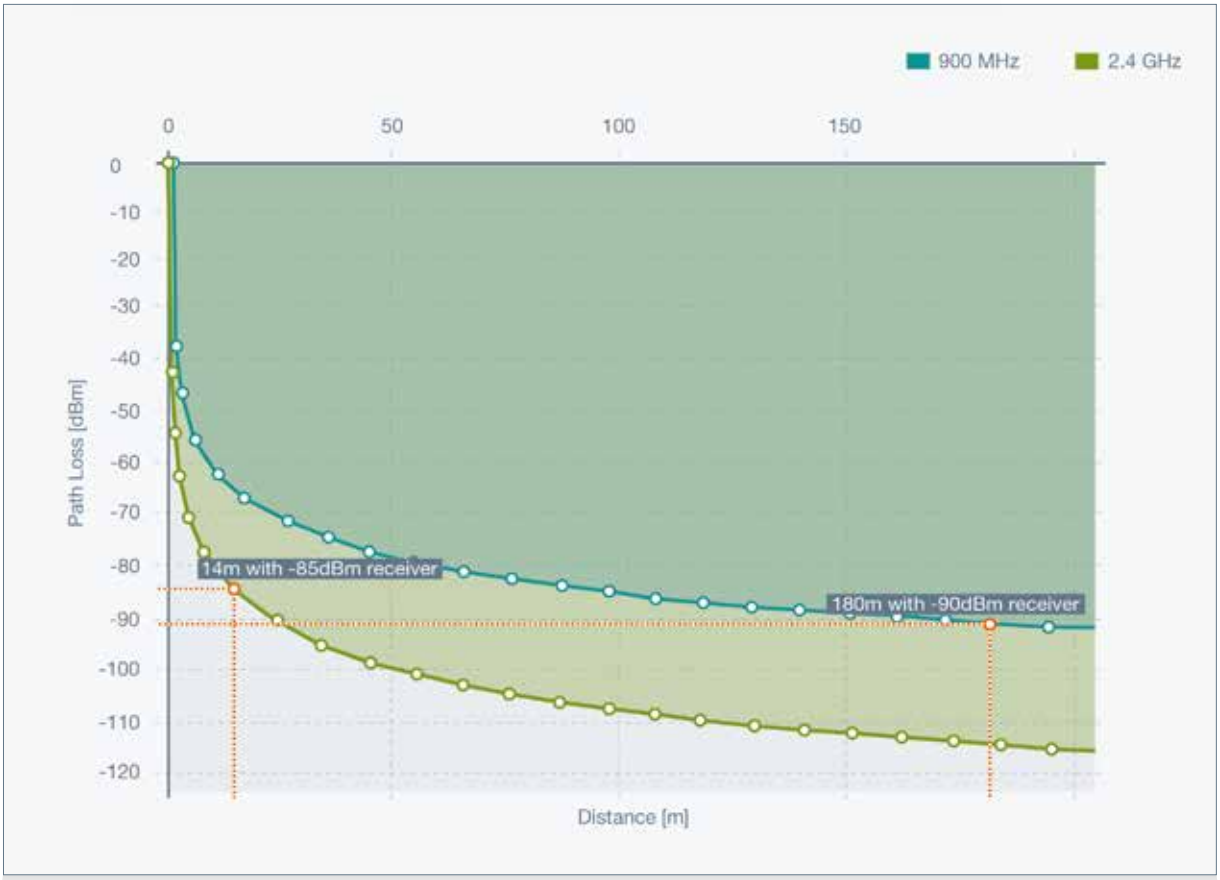


Figure 5: Real propagation in a shadowed urban environment (path loss exponent of 3.7)

The figures show the difference of the theoretical free space propagation and the practical propagation in a shadowed urban environment with a path loss exponent of 3.7. Comparing the theoretical free space propagation and the practical propagation in a shadowed urban environment at 2.45 GHz, it can be seen that the theoretical distance of 175 m with a receiver of a -85 dBm sensitivity shrinks to just 14 m. Comparing the two curves at 900 mHz, the theoretical distance of 850 m with a receiver of -90 dBm sensitivity decreases to 180 m.

1.2.3 REASONS FOR SHORTER DISTANCE IN A REAL ENVIRONMENT

1.2.3.1 Penetration of obstacles

Now, as radio waves are basically the same as light, the propagation of radio waves is the same: linear. But due to the different wavelength, some effects have a different intensity. Light obviously penetrates glass or any other transparent material very well but it is totally blocked by a brick wall. It can partly penetrate thin paper or, depending on the power of the light source, thin cardboard. It is able to bend very slightly around the edges of obstacles, which is seen as a half shadow. Light is totally reflected on some surfaces, like polished metal or mirrors, and only partly reflected by other materials.

Radio waves are similar, but the limits are not the same. The lower frequency or longer wavelength allows radio waves to penetrate material easier, so a brick wall is not necessarily an absolute obstacle; however, similar to light penetrating the paper, the intensity of the radio waves are damped. Also sound waves can be bent more easily around obstacles. The rule is, the lower the frequency, the easier the wave penetrates obstacles. Independent of the wavelength, a radio wave is always reflected by a metal surface.

1.2.3.2 Reflection

The effect of metal always reflecting a radio wave is very important to consider in industrial environments. It means that a metal obstacle will not be penetrated. The same is true for a metal-reinforced concrete wall since the steel acts as a shield. The reflected wave is phase-shifted by 180°.

Reflection also has another effect. Depending on the angle that the wave hits the reflecting obstacle, the wave can be reflected by the surface and reach areas via this detour.

1.2.3.3 Bending around obstacles

When a wave hits the corner of an obstacle that is large in comparison to its wavelength, it bends. This means the waves also propagate behind the corner of the obstacle where there should be a shadow or dead space.

1.2.3.4 Diffusion on obstacles

Diffusion is created when the radio wave hits an obstacle that is small in comparison with its wavelength. The signal is divided into multiple weaker signals that propagate in all directions (see figure 6).

1.2.3.5 Interference

All effects of reflection, bending, and diffusion create new waves that interact, amplify, or nullify each other.

Figure 6 shows this principle. But in the real world, all reflections, diffusions, and bendings interact and create patterns showing areas of good signal strength and areas with bad signal strength. This is called interference. The consequence is that on one point the signal can be received, but just a short distance away from this point the signal can no longer be received.

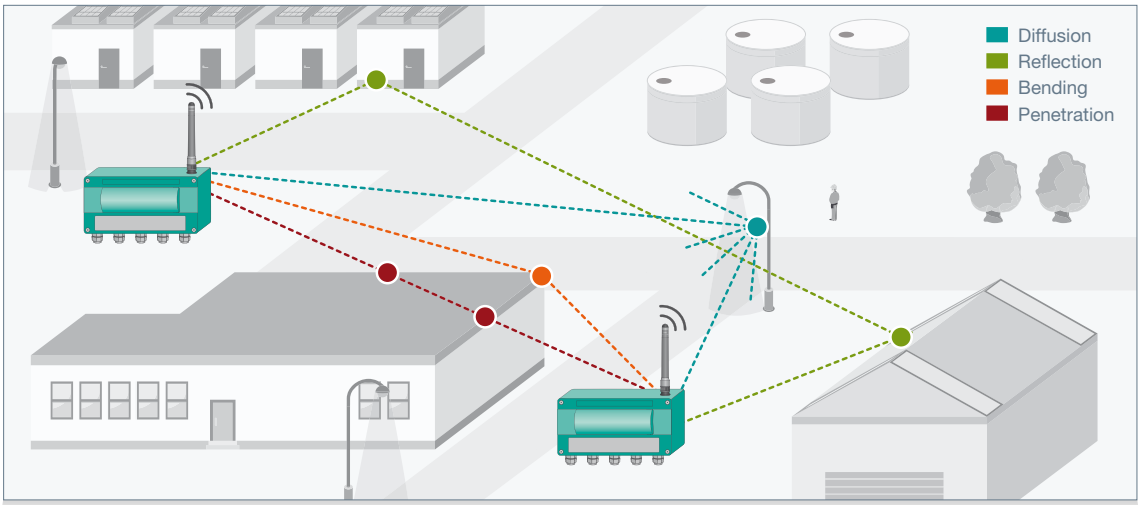


Figure 6: Diffusion, reflection, bending, and penetration of obstacles

Figure 7: Positively superimposed wave, constructive interference

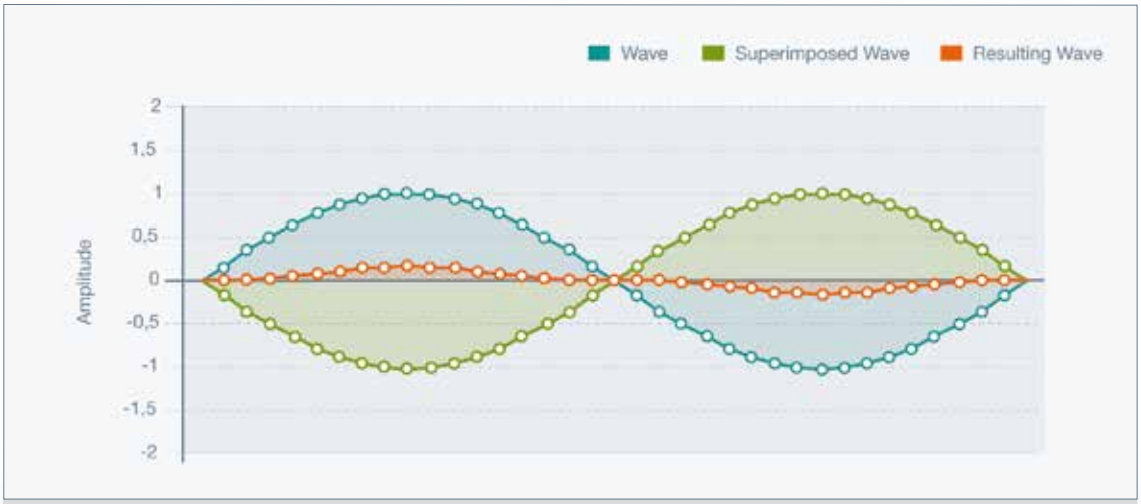


Figure 8: Negatively superimposed wave, destructive interference

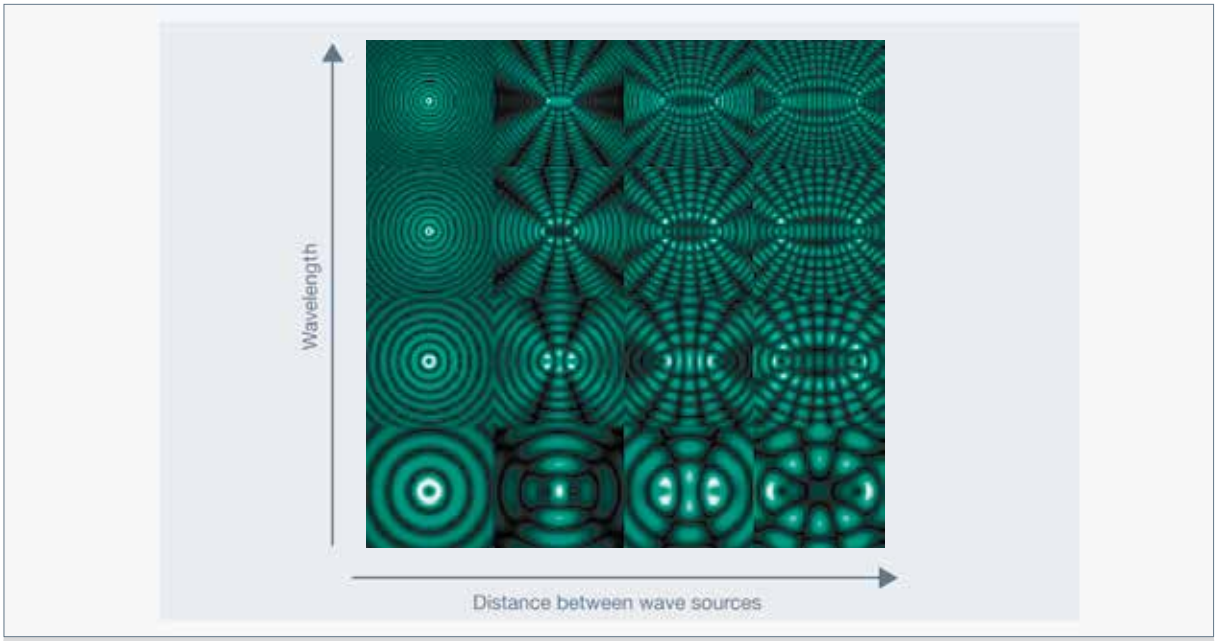


Figure 9: Interference of two circular waves, dark areas destructive, light areas constructive interference (Author: Florian Marquardt (Ludwig-Maximilians-Universität München))

1.2.3.6 MultiPath Fading

Radio waves can be negatively affected by reflections. When the radio wave is reflected one or more times on one or more obstacles, the resulting wave takes multiple paths to the receiving partner. This can result in canceling the signal at the receiver or destroying the signal in another way. Also, the original signal can arrive at the receiver slightly time shifted. This can also happen if the sender and receiver are relatively close to each other. The result is that the receiver does not recognize the signal in a proper manner.

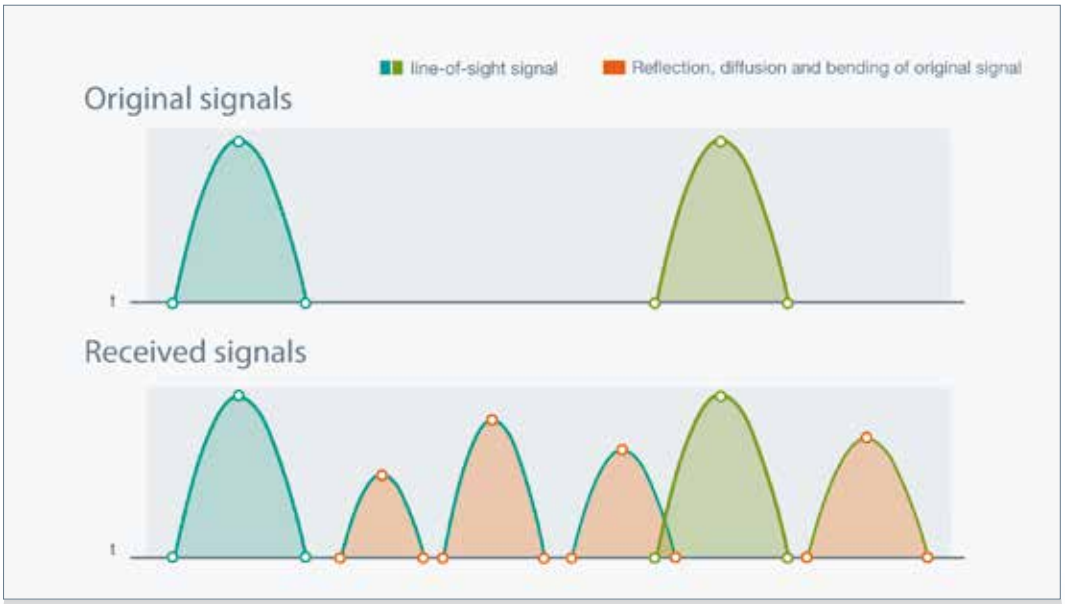


Figure 10: Receipt of the original signal and its reflections, bendings, and diffusions

1.2.3.7 Fresnel Zone

Based on data presented in the preceding pages comparing light and radio waves, a line of sight can always support a reliable connection. This is not always the case.

d [m]	b [m] 900 MHz	b [m] 2.4 GHz
10	0.913	0.559
25	1.443	0.884
50	2.041	1.250
100	2.887	1.768
150	3.536	2.165
200	4.082	2.500
250	4.564	2.795

In order to make this connection reliable and stable, the Fresnel zone must be considered. Fresnel zones are rotational ellipsoids which are formed between two antennas. For practical use, only the first Fresnel zone is important since the majority of energy is transferred here. Therefore, the space within the first Fresnel zone should be free of obstacles. When obstacles reach into the Fresnel zone and cover half of the area, a damping of up to 6 dB is added. This is important to know when setting up devices in the field: the line of sight must have enough space surrounding it.

Here the center radius of the first Fresnel zone is given in a table for 900 MHz and 2.4 GHz. This zone should be kept free from obstacles.

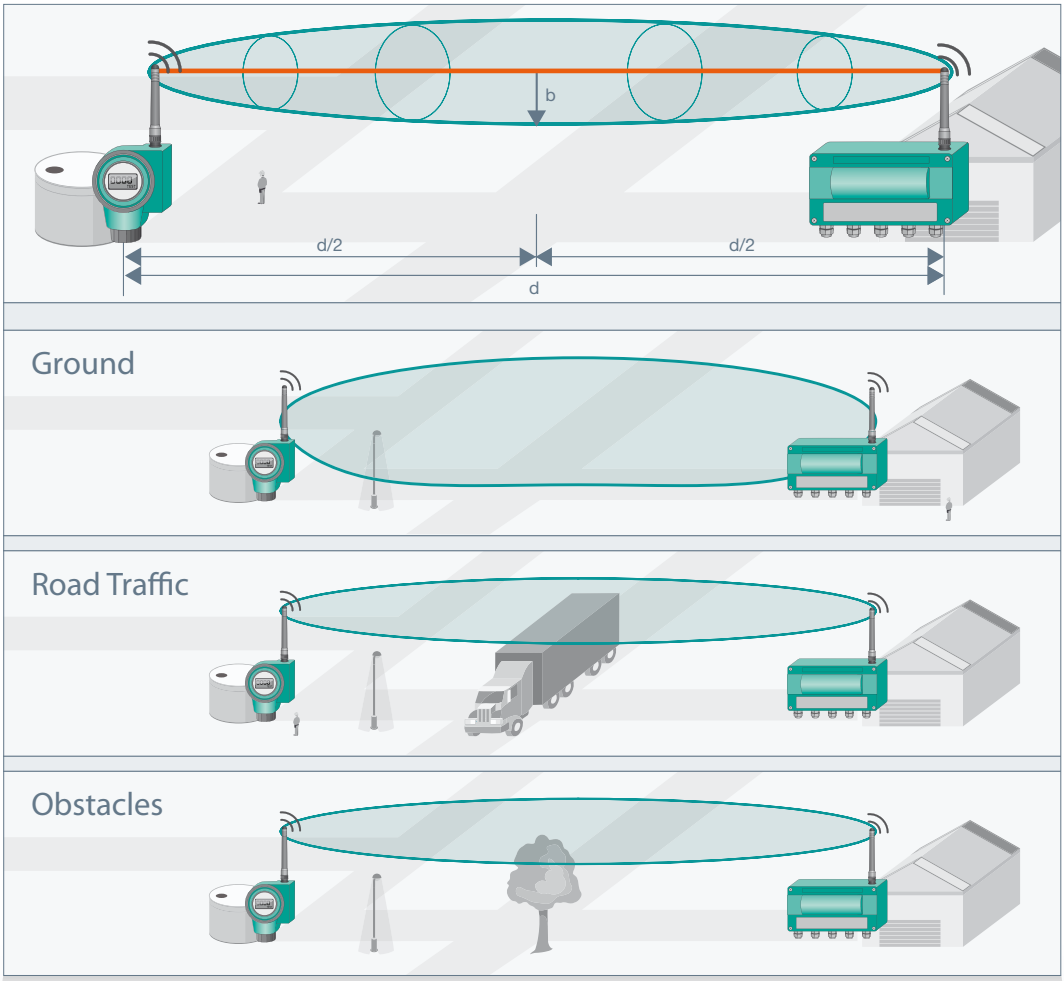


Figure 11: Fresnel zone and possible disruptions

1.2.4 CHANGING ENVIRONMENT

Static objects are of great concern to radio communication; however, moving objects are equally important in an industrial application: Trucks drive through, mobile equipment is moved back and forth, and temporary installations are erected and torn down. All of these environmental changes affect wave propagation. This results in a radio connection that works intermittently. If known, it is important to deal with these issues.

The other conditions that may occur are changes in the RF environment, and they may not be controllable. As described, radio waves are part of the electromagnetic spectrum and share the same medium, the open space. It is impossible to control what happens in this space. Use of mobile radios, cell phones, or WLAN laptops are running for commissioning and maintenance, and frequency converters with high transients, as well as welding machines are operating and radiating their energy. Microwave ovens can jam the 2.4 GHz frequency band, and even the weather can influence performance. Humidity condensing on an antenna can decrease its performance. All of these conditions can influence communication and are continuously changing.

1.2.5 CONCLUSION

This results in some guidelines when starting wireless communications:

- A line of sight between communication partners is always desirable.
- If a line of sight is not practical, the obstacles should not be massive and the partners should be more to the edge of an obstacle to allow the wave to bend around it.
- Paths for mobile equipment and transport vessels should be considered and controlled.
- Metal can be a benefit or detriment. It can either amplify or nullify the wave.
- Due to the interference of reflections and multipath fadings, moving the antenna a few centimeters can help.
- Frequency management should be applied as part of administration since multiple networks might “pollute” the background electromagnetically.

2.1 MODULATION

The radio wave itself carries no information. The process by which the information is attached to the wave is called modulation. There are several analog and digital modulation techniques. The most well-known analog technique is amplitude modulation. The carrier wave is overlaid with the signal wave.

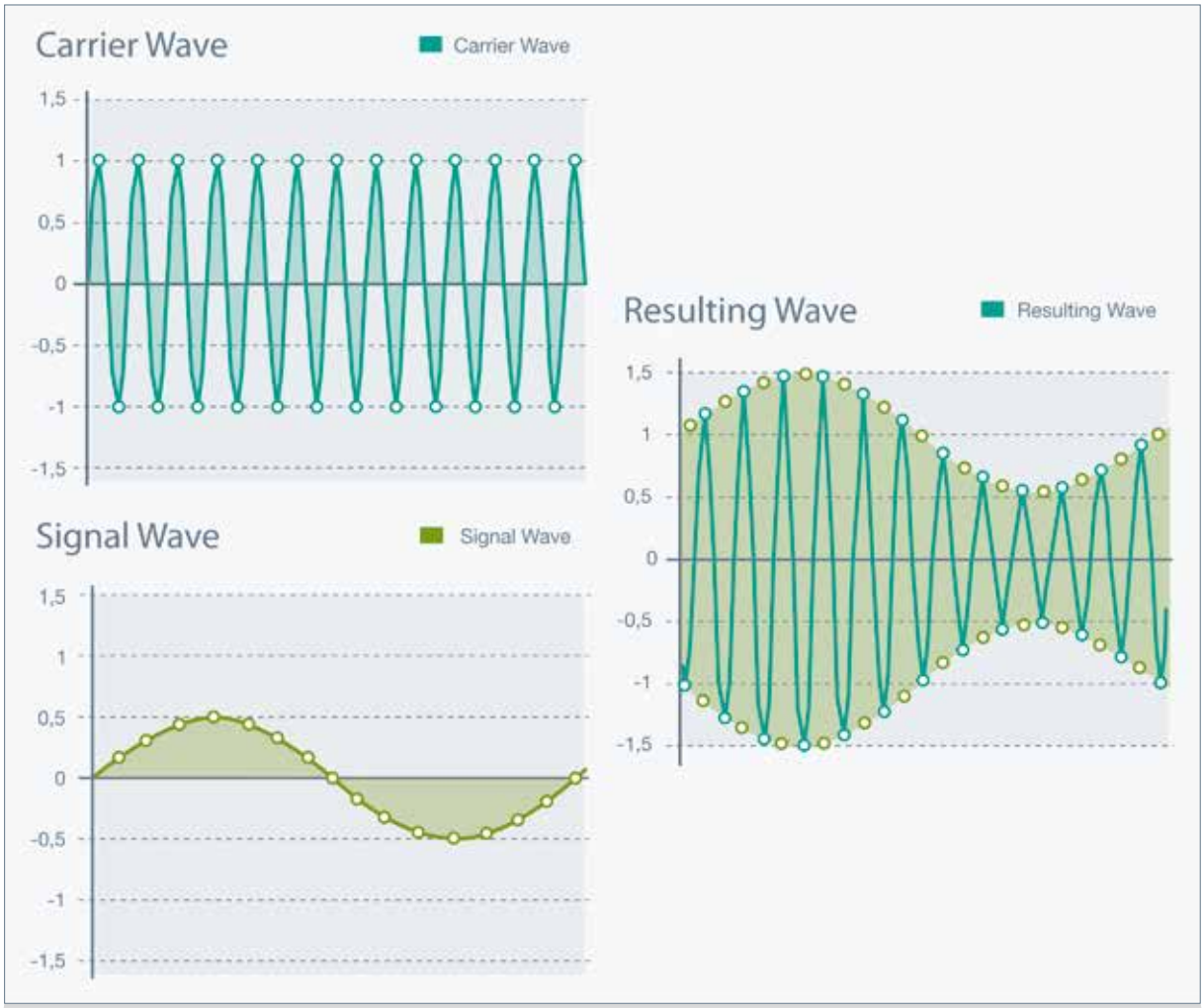


Figure 12: Amplitude modulation – carrier wave, Signal wave, and resulting wave

Since digital electronics and information technology have evolved, other, more effective ways of digital modulation have been developed. There are currently two state-of-the-art methods which are mentioned quite often and should be understood. Both are frequency spread methods, where a small bandwidth signal is spread to a wider bandwidth. This distributes the energy of a signal to a wider frequency spectrum. The result is that the amplitude of the signal, which is now distributed over a larger frequency range, is lower and, therefore; “blurred” in front of the background noise. The advantages are a better tolerance to narrow band jamming and a more secure transmission since the signal is harder to detect by other systems.

2.1.1 FHSS

Using the frequency hopping spread spectrum (FHSS), the single message packages are each sent on different frequencies where the sequence of selected frequencies is distributed in a quasi-random fashion over the entire frequency band.

The single messages are on a narrow bandwidth. Nevertheless, since the sequence of the single transmissions change, the communication still uses the entire bandwidth.

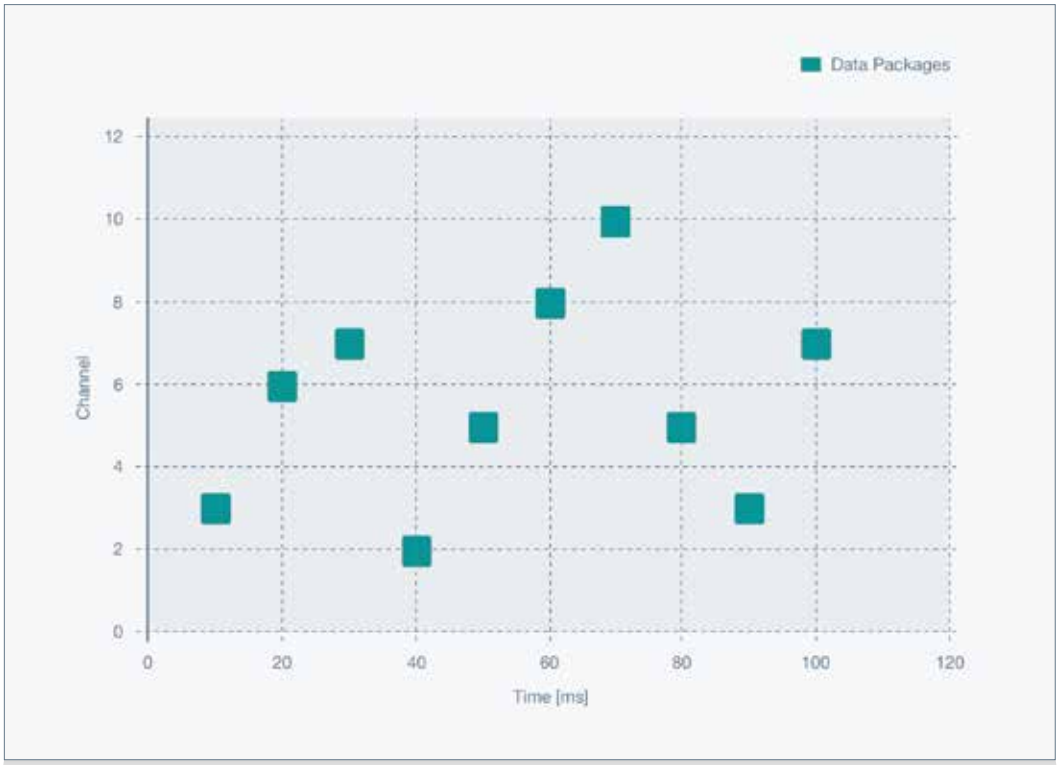


Figure 13: Frequency hopping spread spectrum

FHSS is used by Bluetooth (see 3.2.2).

2.1.2 DSSS

In the direct sequence spread spectrum (DSSS), the message is multiplied with a digital sequence, the spread key, which has a higher bandwidth than the message itself. Therefore, a higher bandwidth is necessary for transmission, but with less energy.

Figure 14: Direct sequence spread spectrum

The lower energy reduces the jamming effects of other wireless systems and the message is “blurred” in front of the background noise. Therefore, it is harder to detect by unauthorized receivers. It can only be retrieved when the receiver has the same spread key for decoding.

Example:
Set the spread key at 10110101 and the bits “1” and “0” will be transmitted. Then, instead of the actual bits, the bits multiplied with the spread key are sent.

Signal	1	0
Spread Key	10110101	10110101
XOR	01001010	10110101

Instead of 2 bits, 16 bits are transmitted. A redundancy is created since the same bit is now contained in 8 bits.

The decoding on the receiving side works the same.

Signal	01001010	10110101
Spread Key	10110101	10110101
XOR	11111111	00000000

Through integration and norm, the resulting bits “1” and “0” are received. Even bit errors can be corrected as long as the sum of the bits is larger than a certain threshold.

Sometimes a variant called code division multiple access (CDMA) is used. Using this technique, every sender has its own spread key. Since the messages are hidden in the background noise, all senders can send in parallel and can be decoded so the receiver can distinguish all senders from one another.

DSSS is used by WLAN (see 3.2.1) and ZigBee. CDMA is used by UMTS mobile radio and the Global Positioning System (GPS).

2.1.3 CONSEQUENCES OF BETTER MODULATION TECHNIQUES

The result of the modulation techniques is a better communication link. Usually, a receiver requires a certain signal strength to detect the signal. This signal strength should be well above the background noise to identify each sent bit clearly. The modulation signals enable the receiver to retrieve the signal even if its strength is relatively close to the strength of the background noise. The ability to retrieve even small strength signals is described as a system or modulation gain. The system or modulation gain enables longer distances with the same sending power while decreasing the bit error rate (see 4.1) at the same time.

2.1.4 CONCLUSION

New modulation techniques have several benefits

- Digital modulation technologies improve the receiving ability.
- Better receiving ability allows longer distances.
- Wireless communication can become more secure and more resistant against jamming.
- The communication link does not easily jam other wireless communication links.

2.2 ANTENNAS

The most commonly used antenna is a dipole. This is called an omni-directional antenna. The shape is donut-like as illustrated in figure 15.

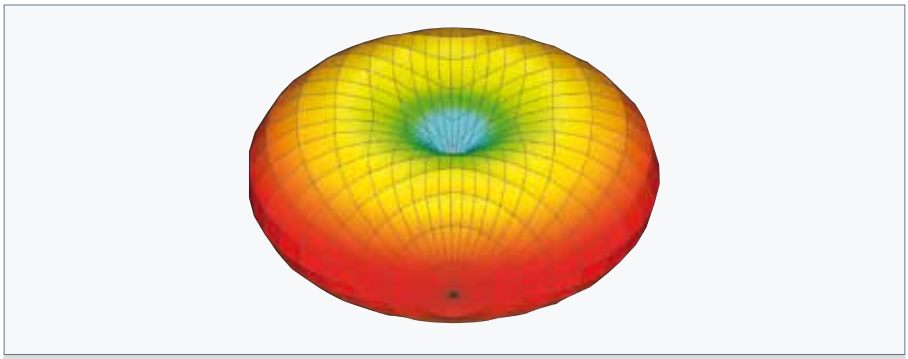


Figure 15: Radiation pattern of undisturbed dipole antenna

This is valid only for an antenna placed in a free room, where no obstacles, and especially no metal surfaces, are in the vicinity of the source. The radiation pattern changes significantly when metal is located in close proximity to the antenna. Depending on the wavelength of the radio wave and the distance and size of a metal surface, the pattern can change as shown in figure 16:

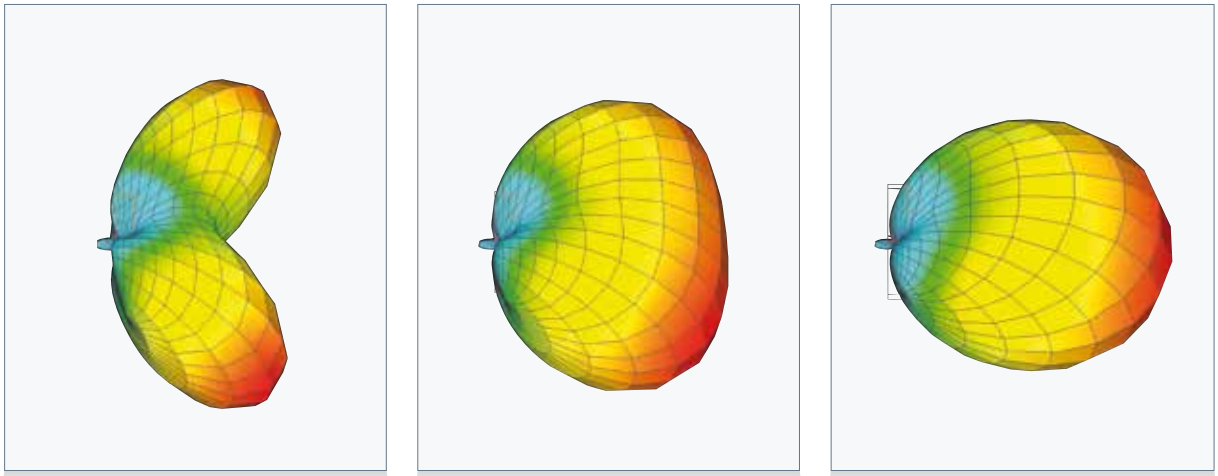


Figure 16: Radiation pattern of dipole with reflective plane in different distances

This illustrates the need to locate the antenna far from metal objects if one wants to generate a signal propagation in all directions. At distances greater than 20 cm to 30 cm, the effects from metal objects become weaker and the radiation pattern starts to revert back to the donut shape.

This effect can be used to get a directional propagation of the radio signal. The effect is used in directional antennas, which focus the signal more in one direction. A metal plate with a calculated size at a defined distance to the dipole will positively reflect the wave and strengthen the signal. With this, the range in one direction can be extended while there is no propagation in other directions. Property must also be considered when placing antennas. Some areas are not covered and a connection cannot be established. Figure 17 depicts this situation:

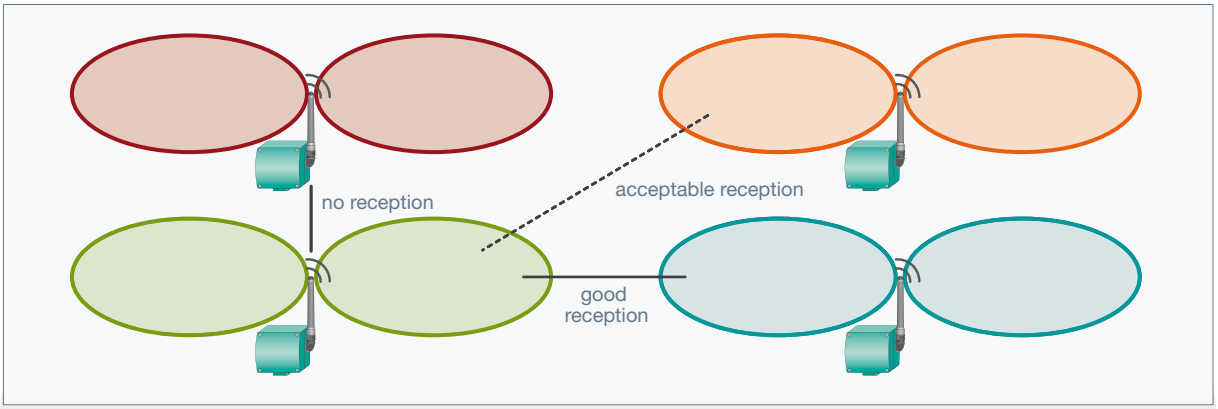


Figure 17: Reception quality depending on radiation pattern and relative position of radios

An omnidirectional dipole antenna has an opening angle of 39 degrees. A good rule of thumb is that the reception is acceptable when the angle is less than 45 degrees.

2.2.1 ANTENNA CHARACTERISTICS

The effects described above, as they are used for directional antennas, are often depicted in a 2D antenna radiation diagram. The two extremes are omnidirectional antennas which radiate equally in all directions, and directional antennas which radiate almost only in one direction.

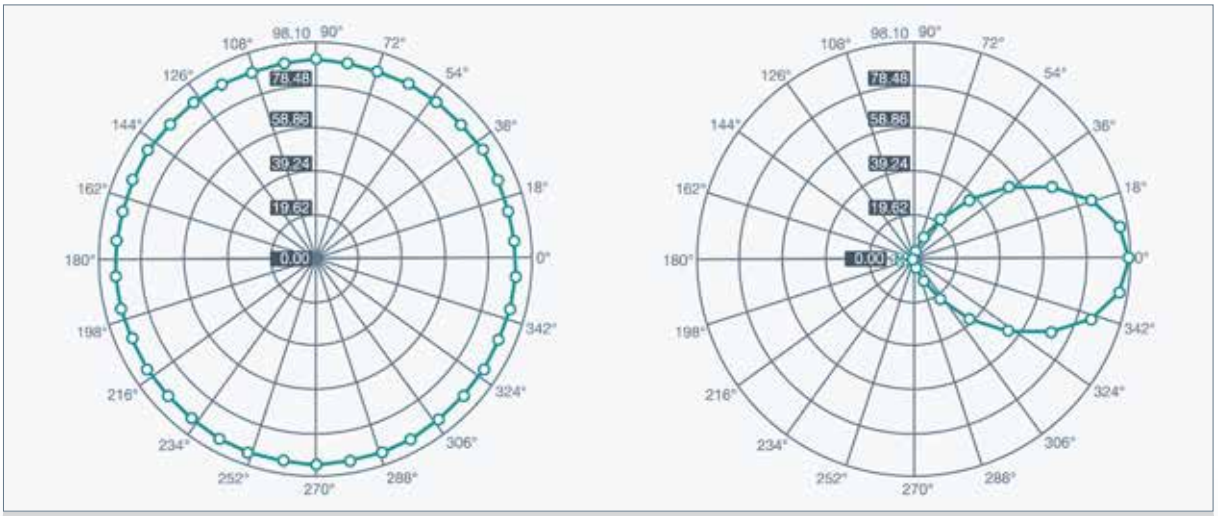


Figure 18: Radiation pattern of omnidirectional and directional antennas

2.2.2 ANTENNA GAIN

The data sheet for antennas contains their gain, given in dBi. This does not mean that the antenna amplifies the input. The factor is relative in relation to an isotropic radiation; therefore, this is also designated as dBi. An isotropic radiation means that the energy radiates equally in all directions. The ideal isotropic radiator is the sun.

Even an omnidirectional antenna radiates only in the plane. The energy is not radiated to the upper or lower direction; therefore, it is more concentrated on a plane. The energy in this direction now is more than it would be if some of the energy would have been radiated to the upper or lower part. A directional antenna focuses all energy into one direction, which improves the performance in the focused direction and decreases the performance in all other directions. A dipole antenna usually has a 1.76 dB higher sensibility (factor 1.5) than an isotropic radiator.

2.2.3 CONCLUSION

Antennas are a vital part of the communication link

- Antennas distribute the signal in a certain pattern.
- Some areas exhibit a strong signal strength, while in other areas, a weak or no signal is found.
- When selecting and mounting an antenna, the pattern must be considered.
- The vicinity of the mounted antenna can change the distribution pattern (e. g., a metal plate close to the antenna).
- Antenna gain is measured by directional focus. This means that the gain is valid only for the area where the antenna distributes the signal.
- Antenna gain works on the side of both the sender and receiver. A high-gain antenna also leads to an increased receiver sensitivity.

2.3 ENERGY SUPPLY

All wireless devices must be powered with electrical energy. This can happen using several options: mains powered, through energy harvesting, or batteries.

2.3.1 MAINS POWERED

An often-used method, especially in wireless office and home installations, is to power the wireless infrastructure with a mains supply and leave the mobile devices battery powered. The obvious advantage is that the energy is virtually infinite and the infrastructure is powered permanently. In a home and office environment, it is not difficult to take care of a mains powered connection. Generally, mains power is available in industrial areas for pumps, fans, coolers, and lighting. It can be an advantage to make use of these power sources when they are located close to the wireless device or to power necessary routers and repeaters in the network.

Nevertheless, this power option is not suitible for mobile devices or for autonomous measurements since a cable connection is still necessary to the device. So it's not really "wireless." Even for this application, the signal line cable can be eliminated, which can be a big advantage, especially when the signal source is located far away from the source.

It must be noted that — if the measurement is of some importance — the reliability of the mains grid should be considered. Sometimes, the power is not installed in a redundant or reliable way since it is a low priority. In this case, a blown fuse would disconnect the power to the wireless device.

2.3.2 ENERGY HARVESTING

Energy harvesting is the collective term for methods which generate electrical energy from other forms of energy present in a certain environment. One of the most well-known examples is a solar cell which harvests the energy of sunlight.

Other energy forms can be transformed into electrical energy:

- Vibration from pumps, motors, fans, moving machine parts, etc., can be utilized by a piezo sensor or a similar mechanical method
- Force from a moving part (e. g., a light switch) can be utilized by a piezo sensor
- Heat from heaters, pipelines, motors can be utilized by thermo elements

Other principles are also possible, e. g., a turbine for pressurized air.

These concepts exist today on paper and in preliminary studies, but the efficiency of these methods is very low (below 10 %). They deliver the energy only during the daylight (solar cell) or when the motor is running (vibration), so they are not a permanent supply.

Due to the low efficiency and due to the fact that environmental energy is not always present, all of those devices must have an energy storage mechanism to store and deliver energy when necessary. Storage is another complexity. One could assume that high-performance capacitors are a solution, but most of them do not withstand industrial environments for long periods due to limited temperature range. The lifetime of a supercap in industrial environments is about 5 years. Accumulators are also very expensive, but could cause problems in hazardous areas, have a limited charge-discharge cycle number, and are almost as expensive as batteries.

Therefore, all energy harvesting concepts today are in a very early stage of development.

2.3.3 GALVANIC CELLS

Galvanic cells are energy converters, generating voltage in an electrochemical way through a redox reaction. The voltage is dependent on the electrode materials used and the type and quantity of the electrolyte. Galvanic cells can be either primary cells (also called batteries) which cannot be recharged or secondary cells (accumulators) which can be recharged.

The properties of a galvanic cell are dependent on the design of the galvanic cell:

- All chemical reactions are temperature dependent, so the selection of materials for electrodes and electrolytes determines the operating temperature range.
- The energy capacity is also dependent on the chosen materials for electrodes and electrolytes and the size of the battery (mass of material used).
- The form of the electrodes can have an influence on the power that can be delivered. Large surface electrodes are able to deliver a higher peak power than small surface electrodes (since the surface for the redox reaction is larger).
- Storage time: the chemistry also determines the possible amount of time a that galvanic cell can be stored without significant loss of capacity.

Figure 19 shows an overview of the properties of different accumulators. It shows the dependencies of material combinations in terms of power and energy density. Lead accumulators (e. g., starter accumulators in cars) have the lowest energy density and power density of the shown accumulators, Li-Ion accumulators have the highest. The green capacitor field is just for reference. The upper half also comprises supercaps.

A large number of wireless devices for home and office such as laptops and cellphones are driven by Li-Ion accumulators. Even if they have a high energy capacity, it is still necessary to reload them once a week (cellphone) or even daily (laptop). Primary cells can give a higher energy capacity and are, therefore, more suitable for devices that work autonomously for a long period of time. The highest possible energy density today is delivered by lithium thionyl chloride. This is a special chemistry which contains 684 Wh/kg and 7,200 W/kg. A D-Cell of 100 g weight contains 68 Wh. When a device requires 10 mW, this is enough energy for 6,800 hours. A year has 8,760 hours, so the battery could power this device for ¾ of a year.

Usually, wireless devices require less average power (1 mW) since they send only at certain intervals (e. g., for 1 s each 10 s), so the battery could live for 68,000 hours or almost 7 years.

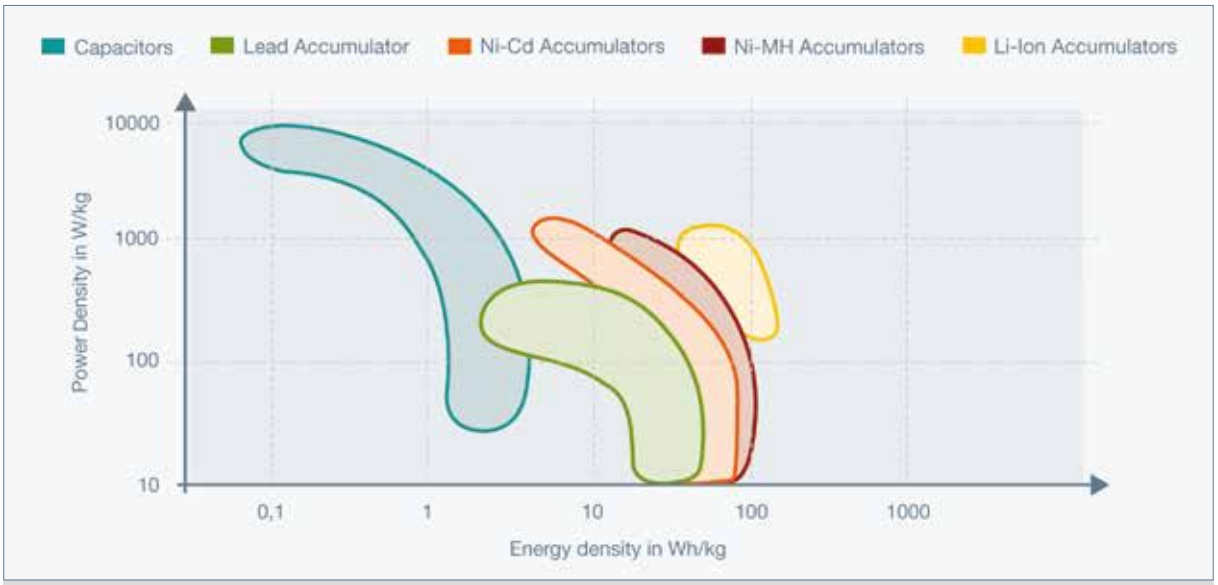


Figure 19: Power and energy density of different battery-types.

2.3.4 CONCLUSION

- Several options for powering wireless devices exist.
- For autonomous measurements, batteries are a good selection and can power a device for years.
- Mains powered devices are good for providing infrastucture for battery-powered devices.
- Energy harvesting solutions are in the early stages of development.

2.4 ENCRYPTION

In contrast to wired communication, where the information is protected from external access and jamming wireless communication can be intercepted, altered, and disturbed since it is transferred via the shared medium of open space. The open space is accessible by everybody, and the interception of information cannot be prevented. However, the transferred information can be protected with encryption.

Encryption is not a new concept. In classical encryption when computers where not available, entire characters or character sets were replaced by other ones. These methods can be deciphered very easily and are outdated and unsecure. For example, shifting the alphabet for a defined offset and then replacing each character of the original text by the new one, can be hacked after 25 tries with brute force or statistically by checking the appearence of certain characters. For example, in english language, the “e” is the most used character. When the “p” in the altered string is the most common character, it can be assumed that in the original text this is the “e” and the code is cracked.

In World War II, mechanical and electromechanical systems where utilized very often. The most famous system at this time was the Enigma, used by the German army to encipher messages. Also, mathematical methods evolved to make encryption more secure.

Modern cryptography started around 1949 where the mathematical base for encryption has been laid. This also ended the need to keep the algorithm of the encryption secret, but leave the security of the encryption only to the choosen key. Another important step was the development of Data Encryption Standard (DES) in 1976 by IBM and NSA (National Security Agency). The DES standard is still used today in Bank Services (e.g. bank cards)

When talking about wireless communication, two major encryption methods exist: WEP / WPA and WPA2 / AES.

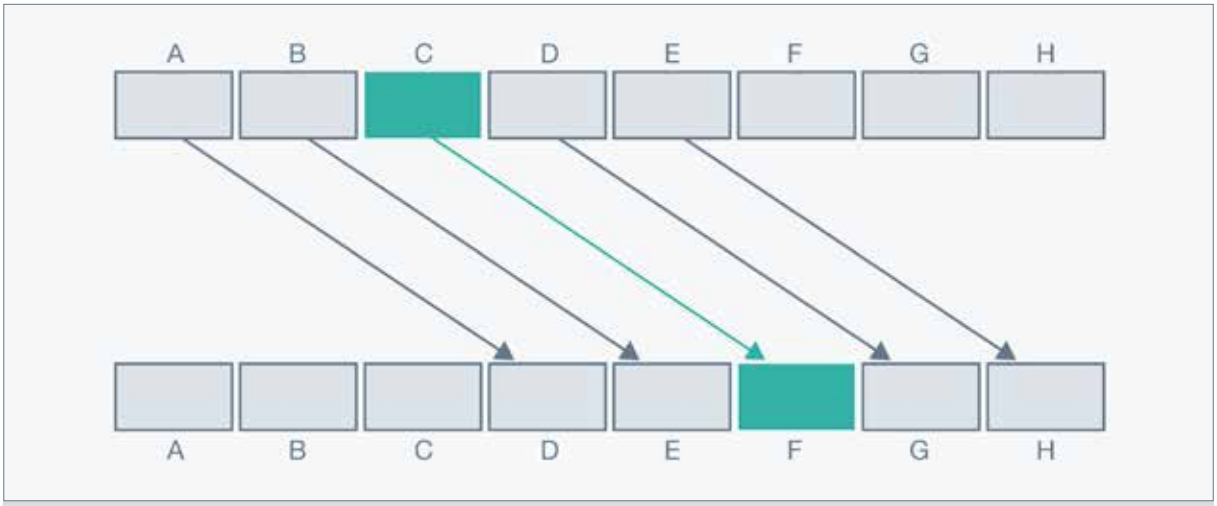


Figure 20: Shift cypher through shifting of 3 characters

2.4.1 WEP AND WPA

WEP was the original algorithm for WLAN. It is a simple XOR operation between the data stream and a pseudo-random, real-time generated stream, called key stream.

During coding at the source, the data stream is combined via XOR with a key stream. This results in the cipher text.

Decoding at the target works the same: The cipher text is combined via XOR with the same key string, which results in the data stream in clear text again.

Source	
Data Stream	...010110001...
Key Stream	...111001010...
XOR = Cipher Text	...101111011...

Target	
Cipher Text	...101111011...
Key Stream	...111001010...
XOR = Data Stream	...010110001...

Table 2: Encryption concept WEP

In order to allow decryption of the message at the receiver side, the key stream must be identical at both the source and target sites. So, the algorithm must be predictable and be the same at both ends of the communication. The algorithm is called RC4. Based on a first key, it generates the successive keys. Of course, the algorithm to generate the keys must be secret in order to make the encryption effective. Due to this and other weaknesses, WEP is unsafe today. Listening to messages for 1 minute and analyzing them for a few seconds reveals the key.

WPA is the abbreviation for “WiFi Protected Access” and is very similar to WEP. WPA has some additional functions like dynamic keys, preshared key (for user authentication), and message integrity check (MIC). Due to the same basic principle, WPA can also be broken within one minute and is not recommended anymore.

2.4.2 WPA2 / AES

Since WPA is not considered safe anymore, WPA2 was created. WPA2 uses a completely different mechanism, it makes use of AES encryption.

AES is the successor of DES, an encryption method invented by IBM in 1976. DES is still in use for bank services. But as DES became unsafe in the late 90s for top-secret government documents due to increased computing power, AES was invented.

AES enciphers a message in blocks with 128 bit length and key lengths of 128 bit, 196 or 256 bit. According to the used key length, AES is called AES-128, AES-196 or AES-256. AES repeats a set of operations several times to encipher a block of 128 bit. The number of those repetitions is more important than the key length. In general terms, one additional round can make the code 10 times more secure.

AES is the most effective and secure encryption algorithm known today. It is certified by the US government to encrypt top secret documents.

There are several possible known attacks, but they all are more theoretical than practical. All attacks known today need up to 2^{100} to 2^{200} operations. A supercomputer with 1 petaflop would need 40.2 million years to perform the best guess, 2^{100} operations. When Moores Law is considered, the effort to break AES is doable in about 100 years.

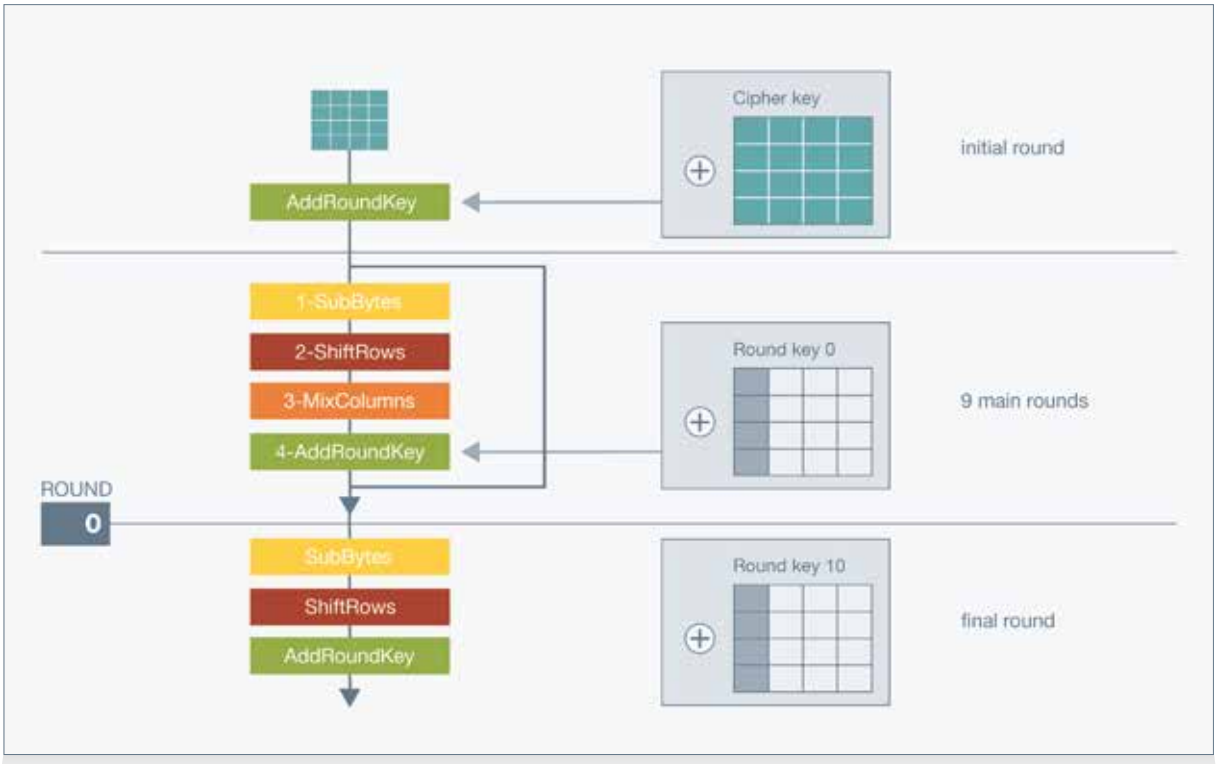


Figure 21: AES encryption process

2.4.3 SPECIAL OPERATING MODES OF ENCRYPTION

AES always enciphers 128-bit blocks of a message, but most messages are much longer. Of course, each 128 bit could be enciphered one after the other with the same key. This mode of operation exists and is called “ECB mode” (electronic code book). But this mode is not very secure. Using the same key again and again can leave a data footprint. To avoid this, AES and other block cipher algorithms use special operating modes.

Counter Mode
Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter." The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual counter is the simplest and most popular.

Cipher-Block Chaining (CBC) Mode
CBC mode of operation was invented by IBM in 1976. In the cipher-block chaining (CBC)-mode, each block of plain text is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plain text blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.

There is a variant of this mode called CBC-MAC which also results in a message authentity code. This code is added to the encrypted message and can be used at the receiving side to check if the message has been altered or not.

Counter-Mode/CBC-Mac (CCM) Mode
CCM combines the counter mode and the CBC-MAC Mode. The Counter Mode part takes care of enciphering the message while the CBC-MAC part works on the integration and authentification of the data.

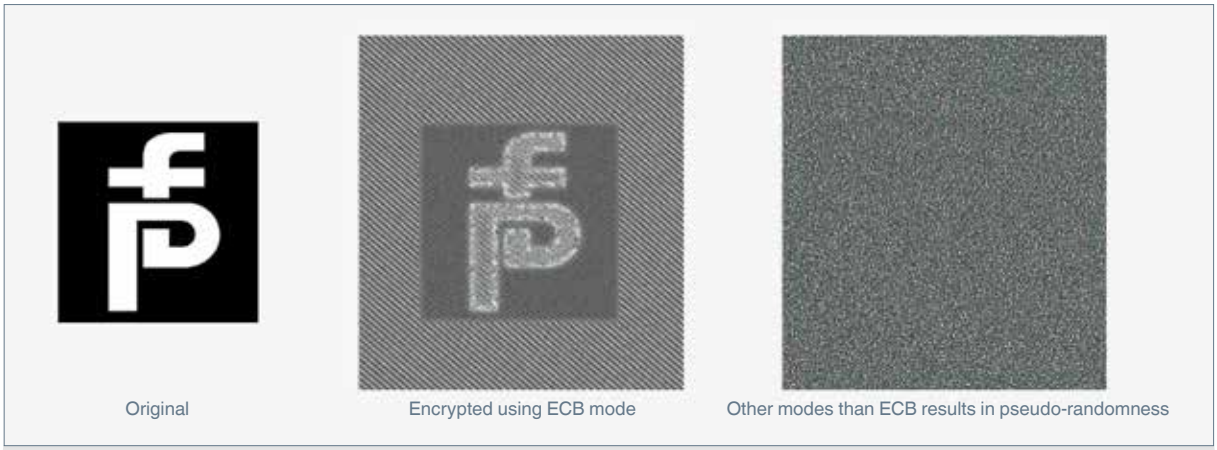


Figure 22: Result of using ECB mode or non-ECB modes for encryption

2.4.4 CONCLUSION

- Several algorithms and methods exist for encryption.
- Especially with the evolution of computer technology and mathematical background, the algorithms became more sophisitcated.
- State-of-the-art algorithms and methods are very safe, virtually unbreakable, and are used to encipher top-secret government documents.

3 REGULATIONS AND STANDARDS

3.1 ISM BANDS

Since radio waves are part of the electromagnetic spectrum and share the same space, regulations must be formed to organize the single frequencies so they do not disturb each other. These regulations are made by governmental authorities and are different in every country.

Figure 23: Frequency bands

The frequency range is divided into bands which cover a part of the spectrum. For example, a frequency between 30 to 300 MHz is called the VHF band and is mainly used for sound broadcasting. This band is further divided into single channels. Your favorite radio station, for example, is on a designated channel in the VHF band.

In order to operate within a given band, application must be made and authorization granted by an organization who oversees the process. However, some bands are held free and can be used by anyone without getting any special license. These bands are called ISM bands (Industrial Scientific Medical). Two major ISM bands that are common are 800 – 900 MHz and 2.4 GHz.

3.1.1 800 – 900 MHZ

The sub-GHz range between 800 – 900 MHz is further divided and slightly different in every country. Therefore, no worldwide standardized product is available. Also, the application of such a radio must be carefully checked to verify that it is in accordance with local regulations.

3.1.2 2.4 GHZ

The 2.4 GHz band is the only free worldwide license band. This makes it perfect for worldwide standards. For example, Bluetooth and WLAN work in this frequency range, this range also allows you to use your laptop or Bluetooth device almost anywhere in the world.

3.2 WORLDWIDE STANDARDS

As the 2.4 GHz band can be used almost anywhere with just differentiation of allowed sending power (1 mW, 10 mW or 100 mW), standards have been developed to enable interoperability of devices. The standards have been created by IEEE (Institute of Electrical and Electronics Engineers). The group dealing with LAN communications is IEEE 802. Based on this, several substandards have been developed.

Basically, all of the standards define the physical layer (the frequency band on which to send, the channel distribution and usage), the modulation, and the Media Access Layer (the method by which participants communicate and are addressed).

3.2.1 IEEE 802.11 (WLAN)

IEEE 802.11 and its extensions, which are designated by characters (e. g., 802.11 g) describe a radio standard for local wireless communication. This is the base standard for the well-known and widely used wireless local area network (WirelessLAN, W-LAN, WLAN).

The name, wireless local area network, comes from the application where a location of a certain area is covered with a wireless network to save on cabling. One can see where a WLAN access point is installed in public places, such as airports, public buildings, and local shops. The entire airport or certain areas of the airport provide a wireless infrastructure and can be used to access the internet. To enable this, WLAN is optimized for increased sending power and ranges with a higher data transmission rate.

WLAN is using DSSS as explained in chapter 1.3.2. The bandwidth of a WLAN signal is 22 MHz. Due to the fact that the distance between two center frequencies is specified in IEEE 802.11 b/g to 5 MHz — only one channel can influence another one. For example, the center frequency of WLAN channel 1 is 2.412 GHz. So the frequency spectrum is 2.401 GHz ... 2.423 GHz. Channel 2 uses 2.417 GHz as the center frequency and the spectrum is 2.406 GHZ ... 2.428 GHz. Since both spectrums overlap, this prevents all channels from being used simultaneously.

The time until a channel is established or an access point has been changed is relatively long. For moving objects, this can cause significant waiting times.

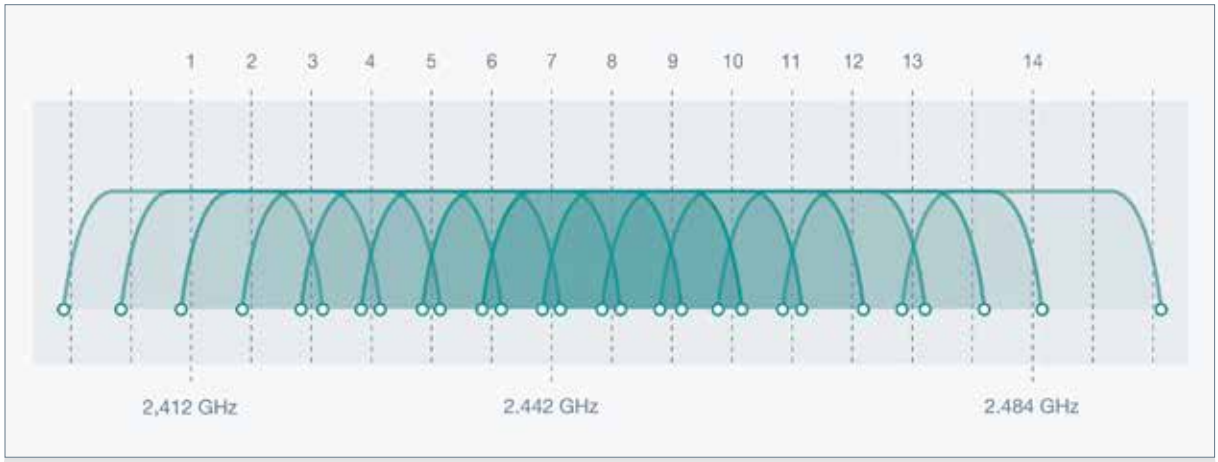


Figure 24: Channel designation in 2.4 GHz band according to IEEE 802.11

Furthermore, with a high population of communication partners, the residual time for each is limited quite strictly. A new communication partner can be active only when the preceding finishes communicating and releases the channel. This occurs when the communication speed begins to slow down.

3.2.2 IEEE 802.15.1 (WPAN/BLUETOOTH)

The IEEE 802.15 is the base for wireless personal area networks (WPAN). Here, the range is smaller than for WLANs, and it is generally just a few meters. The first sub-standard IEEE 802.15.1 is known as Bluetooth. The term WPAN is also relevant. For example, a Bluetooth headset used for a cell phone has a range of only one or two meters. The cell phone can be carried in a pocket and be operated through the headset. So it is a personal network, just for the cell phone user and with higher sending power, the range can be extended.

Bluetooth is also able to transmit at relatively high data rates even if they are less than WLAN. Also, Bluetooth has lower power consumption than WLAN.

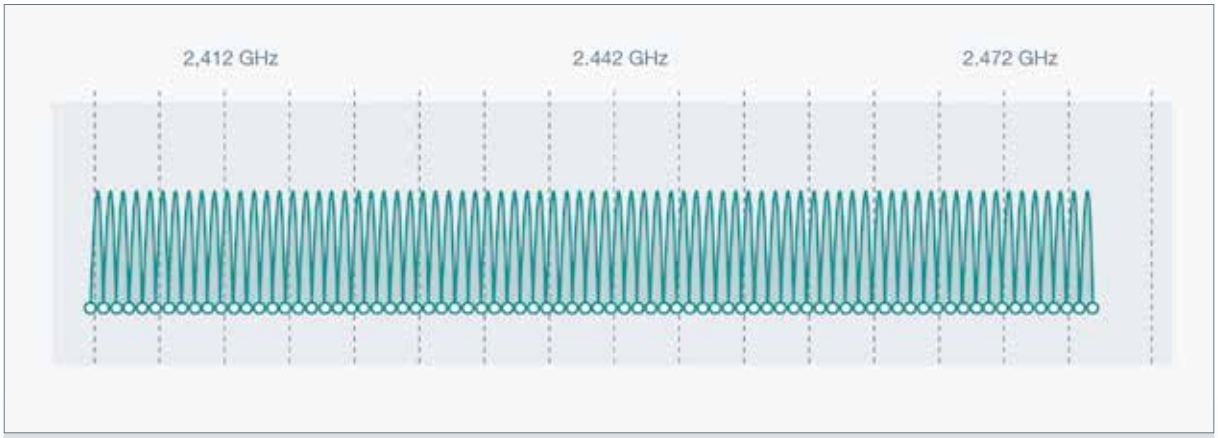


Figure 25: Channel designation in 2.4GHz band according to IEEE 802.15.1

Bluetooth or IEEE 802.15.1 divides the band into 79 channels each with a channel width of 1 MHz and changes between the channels up to 1600 times per second. The resulting spectrum is illustrated in figure 19 (the WLAN channel center frequencies are also shown for better orientation).

3.2.3 IEEE 802.15.4 (LOW RATE WPAN/ZIGBEE)

IEEE 802.15.4 is another substandard of IEEE 802.15 and deals with low data rate WPANS.

Even if Bluetooth is better in power consumption and has less data rate than WLAN, it is not suitable for some applications. In some applications, only a small number of status bytes must be transmitted, but they must be transmitted at a relatively fast rate. Since autonomous operation of this battery-powered device is desirable, and to enable the battery to last a reasonable time, the power consumption of such a solution must be optimized.

The most commonly known implementation of this is ZigBee. This solution is implemented for building automation where just a switch or temperature setting must be transmitted for a light to be switched on or the desired temperature to change. The information here is very limited. In fact, the temperature could easily be coded in 2 bytes. Also, these operating elements could be battery powered with the battery lasting 10 years. Even with small energy harvesting devices, a totally maintenance-free solution is possible.

Figure 26: Channel designation in 2.4GHz band according to IEEE 802.15.4

As in WLAN, and according to IEEE 802.15.4, wireless technology also uses DSSS as a modulation scheme. In contrast to WLAN, however, 802.15.4 divides the spectrum into 16 channels with a channel width of only 2 MHz (Figure 26). Due to the smaller channel width, these are 16 non-overlapping channels; however, the possible data throughput is also reduced.

3.2.4 COMPARISON

In general, wireless networks can be grouped into WPAN (wireless personal area network), WLAN (wireless local area network), WMAN (wireless metropolitan area networks) and WWAN (wireless worldwide area network).

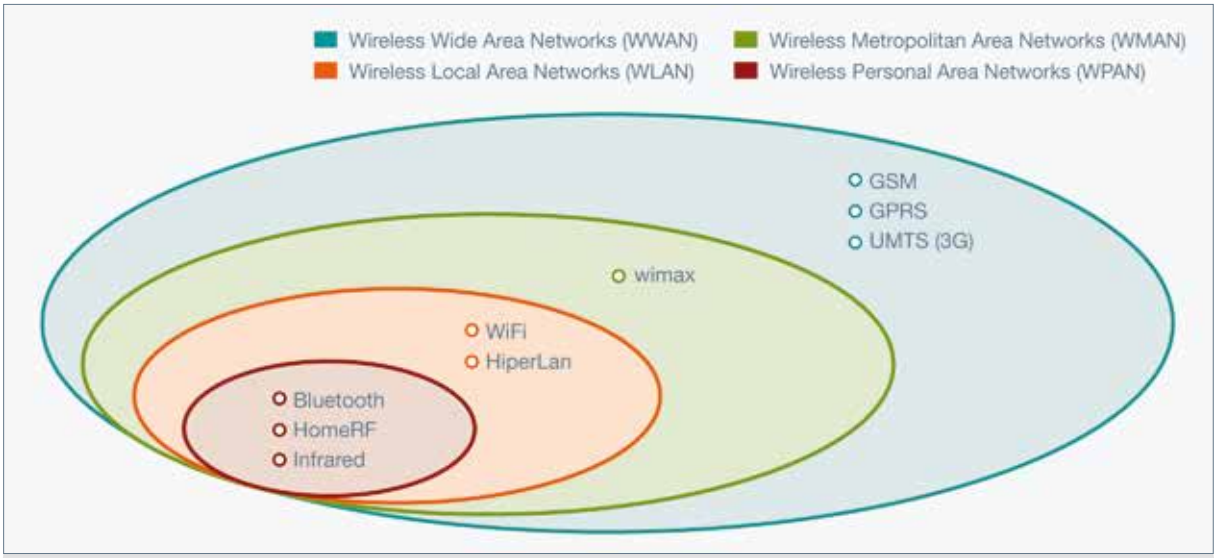


Figure 27: Standards for WPAN, WLAN, WMAN, and WWAN

As implicated by their names, the properties of these solutions in terms of range and data rate are optimized for personal, local, metropolitan, or worldwide coverage and use.

The properties in terms of data rate and range can be shown as follows:

Figure 28: Wireless standards and their properties with respect to range and data rate

3.2.5 COEXISTENCE

In a real-world environment, different wireless communication exists in parallel and shares the same transmission medium, the open space. Therefore, they can influence each other. The influence is recognized when single data packages collide and destroy or alter each other. This happens when the following three aspects fall together:

- Time
- Frequency
- Location

Or in other words: When two systems send data packages at the same time on the same frequency in the same location, the packages can collide and destroy each other.

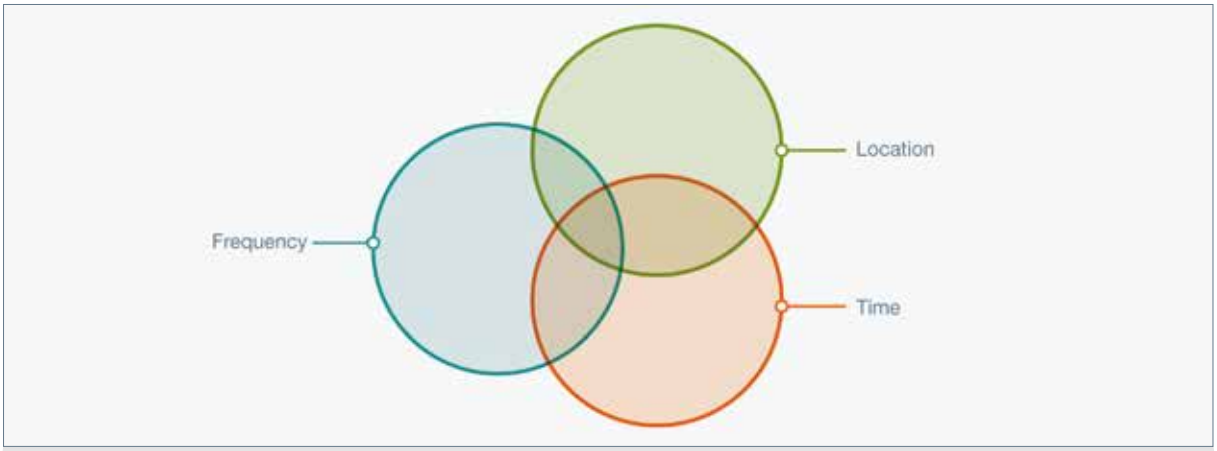


Figure 29: Overlapping of time, frequency, and location causes coexistence problems

Two of those conditions are directly under the influence of a user: Location and Frequency.

When two networks are located close to each other and their range overlaps, this fullfills the condition of "location." The range is mostly determined by the sending power and the environment. The networks do not interefere with each other when they use different bands (e. g., 2.4 GHz and 900 MHz) or if they use different channels within one band (e. g., using channel 1 and 6 according to IEEE802.11). When selecting or blacklisting the channels in a band, it must be ensured that the channels do not overlap due to bandwidth.

Since all the widely used standards use the same frequency band of 2.4 GHz, there is a certain chance that they also use the same channels or overlapping channels. This would fullfill the condition of using the "same frequency." The networks do not interfere if they are out of range of each other. For example, a Bluetooth system covering a small area in one end of a factory will not be disturbed by a WLAN installed at the other end with a range outside the Bluetooth area.

When systems send messages at the same time, this fullfills the condition of “timing.” Timing is not directly under the influence of a user. A system sends messages when needed, and two networks are not synchronized and agree on the timing. But a related aspect is under user control: the duty cycle. As more messages are sent by each system in a certain timeframe, the higher the probability that messages collide. When messages collide, the messages are normally resent, but when both systems have to send and resend many messages in a certain timeframe, the chance to get a message through decreases. As a first step, communication will slow down, which can make the systems unusable for some applications. At a certain point, the traffic is too much and communication is lost completely. Therefore, it is important to check the duty cycle of each system and to estimate if the overall duty cycle of all systems is too high.

Coexistence is assured when at least one of the three aspects is decoupled from the other two. These examples illustrate that proper planning for wireless networks is necessary. This management should consist of a dedicated group of workers in the plant. Installation of wireless networks without first consulting this group must be avoided.

3.2.6 CONCLUSION

- Different wireless standards have different properties.
- Generally speaking, there is a tradeoff between communication speed and communication distance.
- With faster data transmission, the range is lower and vice versa unless other parameters, such as sending power, antenna, or modulation gain, are tuned.
- The wireless standard must be selected in accordance with the application and several aspects, such as battery lifetime, range, and data rate must be considered.
- Due to all the different properties and parameters that can be adjusted, there is no one wireless system for all applications, so every application might need its own wireless system.
- It is possible to set up different wireless systems in the same frequency band.
- Special care and consideration must be taken to ensure proper coexistence.

3.3 NETWORK TOPOLOGIES

Since wireless networks can contain more than two participants, the organization of those networks is of interest. The architectures for the networks include star, mesh, and star-mesh hybrid topologies. Whether a network design is appropriate for the particular application depends on how much and how fast data gets transmitted, the transmission distances involved, battery life, and the mobility and degree of change in the sensor nodes.

3.3.1 STAR

Using star topology, each wireless sensor end point sends data directly to the gateway. From this point, data is sent to other systems. Star networks offer the fastest data gathering speed.

A star topology is a single-hop system in which all wireless sensor nodes are within direct communication range (usually 30 to 100 m) of a base or monitoring station called a gateway. Among wireless-networking topologies, the star consumes the least overall power but is limited by how far the radio transmitter in each node can send. This topology suits installations that require the lowest power consumption over limited geographic range.

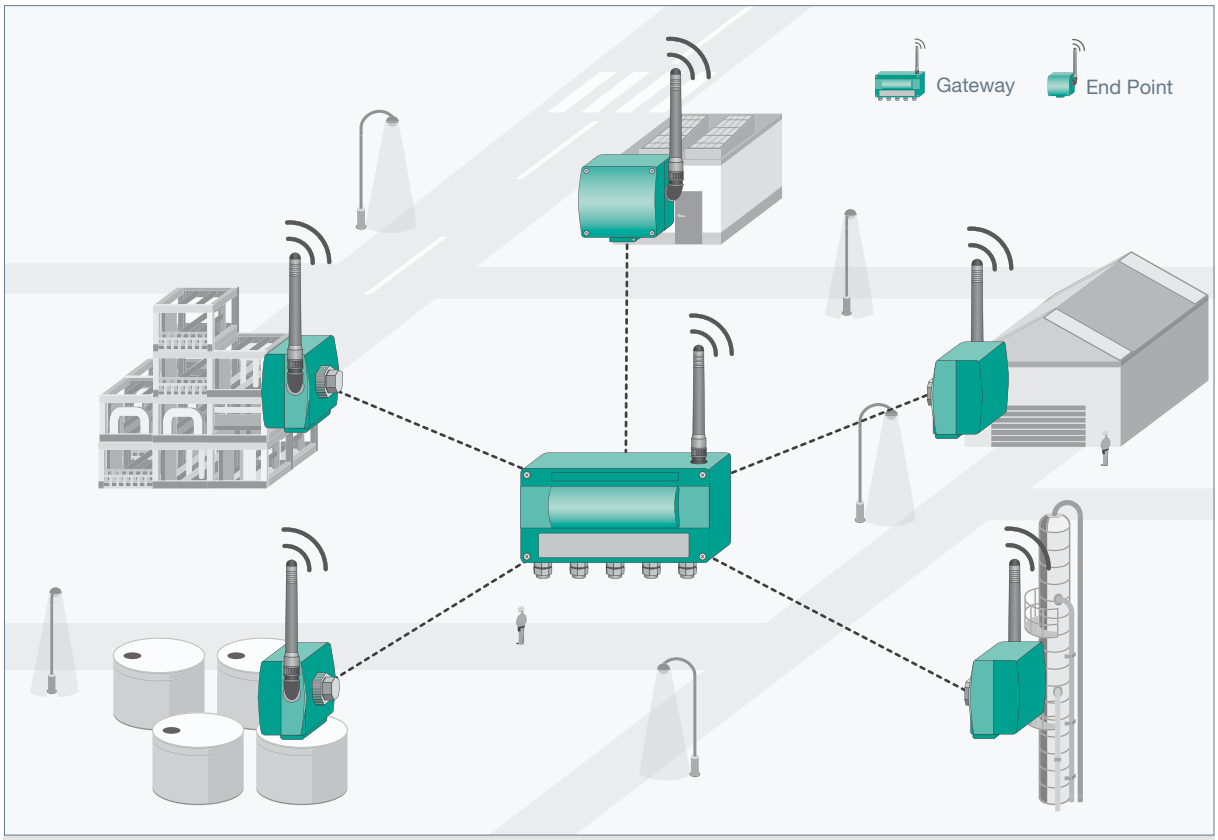


Figure 30: Star network

3.3.2 MESH

In mesh networks, each wireless sensor acts as a router, sending and receiving data from other sensors or the gateway. Self-configuring networks automatically determine the best path for data to take from sensor to gateway. Data is automatically sent around failed sensor routers.

Mesh topologies are multihopping systems. Here, wireless sensor nodes called routers “hop” data to each other and to a base station. The network is self-configuring for the optimum data path of each node. A node failure is recognized and the network automatically reconfigures itself by sending data around the problem. A mesh network is highly fault tolerant because each sensor node has multiple paths by which it can get data back to the base station (gateway) and to other nodes. The multihop technique supports a much longer range than a star topology but consumes more power. This is a consequence of the network’s higher duty ratio. Sensor nodes must always “listen” for messages or for changes in the prescribed routes through the mesh. Depending on the number of nodes and the distances between them, the network may also experience high latency as sensor data hops node-to-node on its way to the base station. This topology is most suitable when there is a premium on high redundancy but node power and battery life are not major concerns.

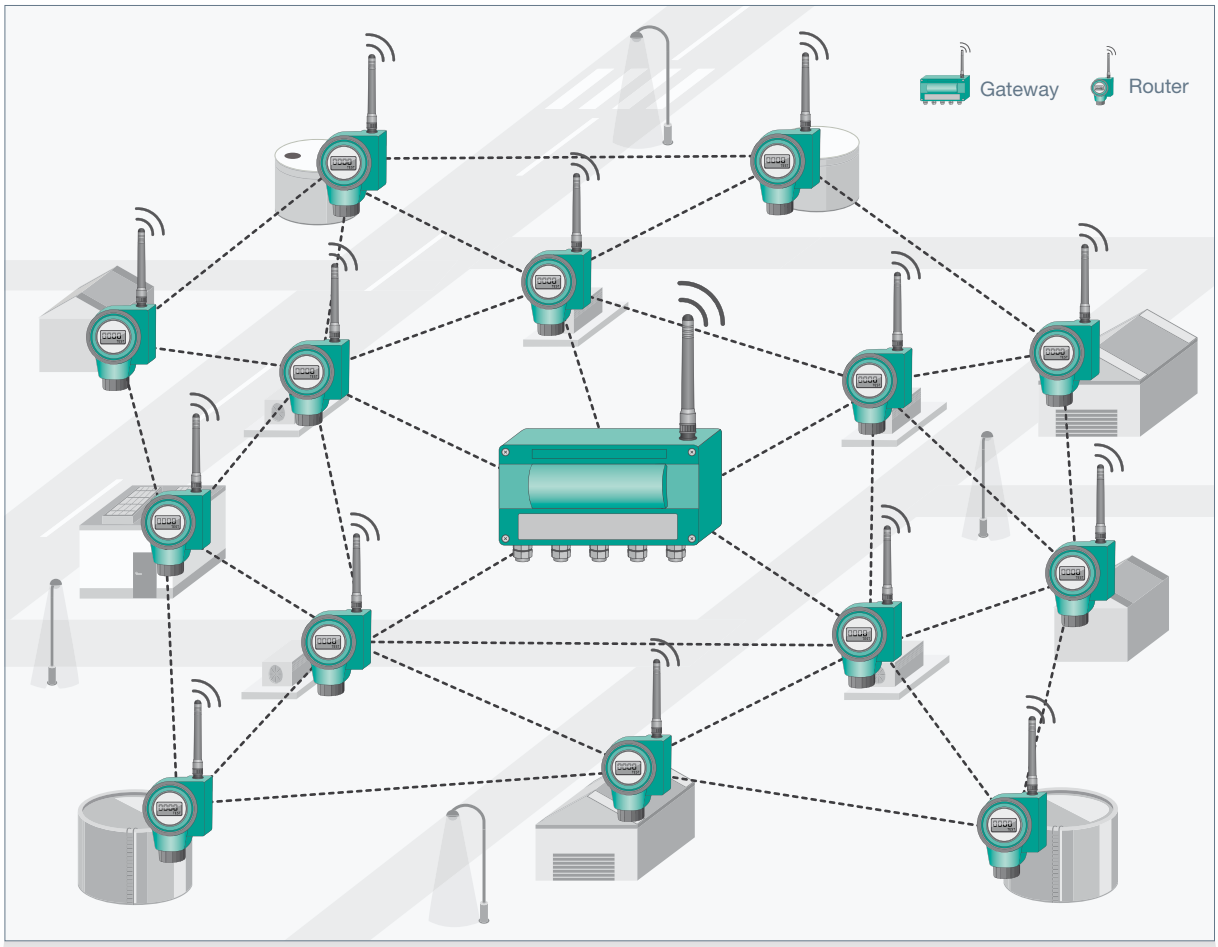


Figure 31: Mesh network

3.3.3 STAR MESH

Star-mesh networks combine star and mesh topologies to gain the speed of the star network with the self-repairing capability of the mesh network. Sensors may be either end points or routers, depending on where they are used in the system.

A star-mesh hybrid topology combines a star network's low power and simplicity with the extended range and self-healing property of mesh networks. A star-mesh hybrid organizes sensor nodes in a star topology around routers or repeaters which, in turn, organize themselves in a mesh network. The routers serve to extend the range of the network and to provide fault tolerance. Because wireless sensor nodes can communicate with multiple routers, the network reconfigures itself around the remaining routers if one fails or if a radio link experiences interference. A star-mesh network offers the highest degree of sensor-node mobility and flexibility for rapid changes to the network. Overall, it consumes the least power for networks that must stretch beyond 30 to 100 m. This topology offers redundant routes all the way to the end points while minimizing end-point power.

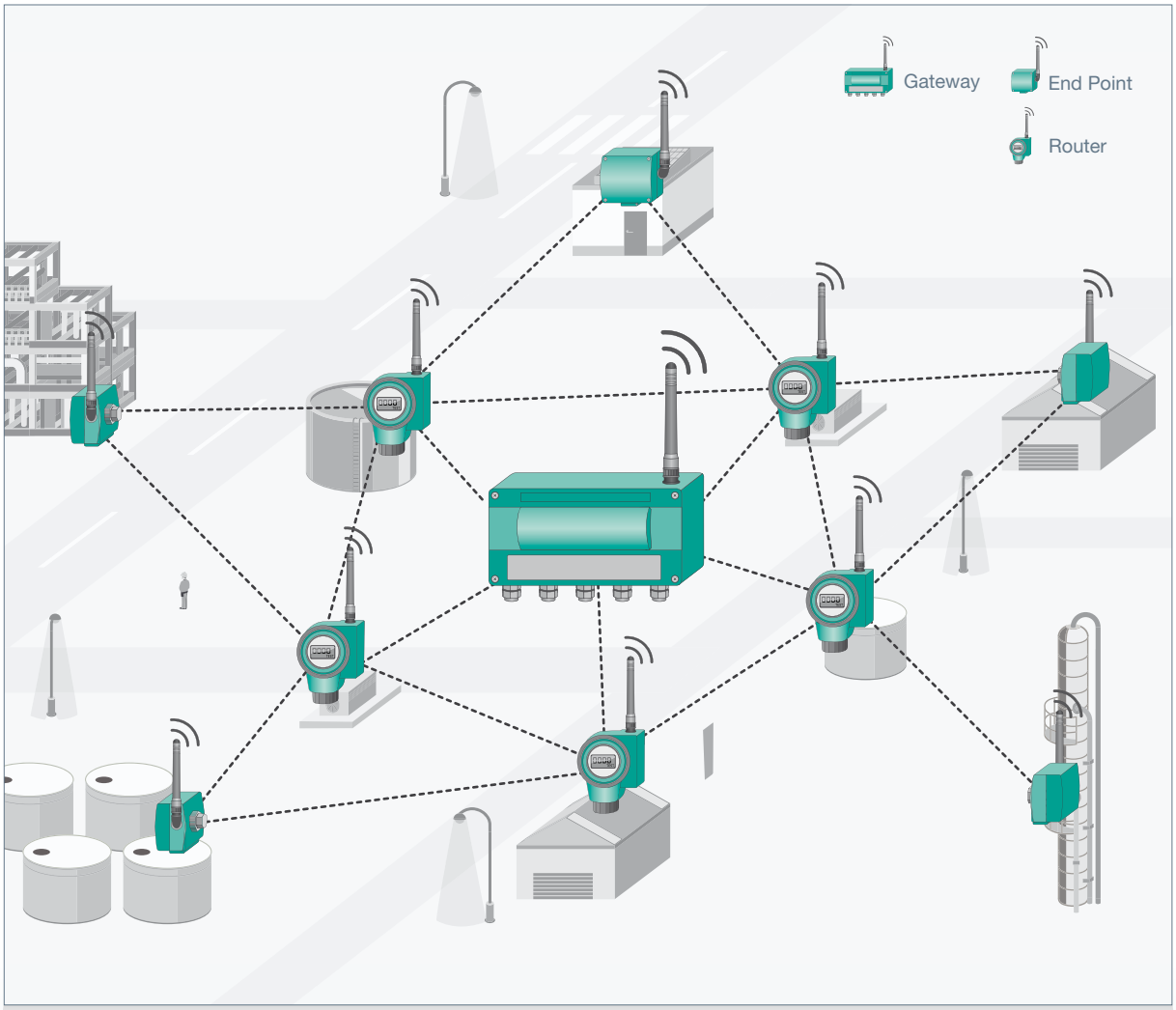


Figure 32: Star mesh network

3.3.4 CONCLUSION

- Wireless networks can be connected in different architectures.
- When applying a wireless system, the architecture must be choosen in accordance to the application.
- If the architectue is not selectable due to the standard, such as WLAN not allowing mesh networking, then selection is not possible and other measures, like allowing multiple access points, must be taken.

4.1 GENERAL CONDITIONS FOR USING WIRELESS TECHNOLOGY

Requirements for communication technology in industrial automation differ from office communication technologies. If a data package is lost in the office world, it is sent again. Usually, the user does not recognize this situation unless the loss of a data package happens so often that almost all packages must be continuously resent. As a result, a slow down of the communication is realized, but this is typically not critical for transferring Excel or Word files. It could cause significant problems if one relies on secure and reliable transmission. If a plant is controlled with a wireless communication system and some data packages are lost, this could cause the process to be interrupted. This is unacceptable. Three main requirements are:

- Latency: the data must be transferred in a defined time frame
- Convergence: the sent and received data must be identical
- Deterministic: The data must be transmitted in a predictable timeframe

The data must be transferred error free in a defined time frame.

To evaluate the single communication technologies used in industrial automation, one can compare the bit error rate. The bit error rate determines how many bits are corrupted statistically.

Medium	Bit Error Rate [BER]
Radio link	10^{-3}
Unshielded telephone cable	10^{-4}
Shielded twisted-pair telephone cable	10^{-5}
Coaxial cable in locally delimited applications	10^{-9}
Fiber optics cable transmission	10^{-12}

Table 3: Bit error rate for different communication technologies

A BER of 10^{-4} is unacceptable for communication systems used in industrial automation. A BER of 10^{-4} means that each 10,000th bit transmitted incorrectly and corrupts the entire telegram. Normally, the corrupted telegrams are not corrected in the receiver but requested again. When a telegram is 128 bytes long (1024 bit) this would mean that each 10th telegram must be repeated, which puts additional load on the bus communication path.

With smooth installations (shielded twisted-pair cable, termination resistor), the BER of industrial communication systems can be improved to be better than 10^{-9}. This would result in repeating each millionth telegram. Sending a telegram each 100 ms this would mean to have 1 telegram repeated per day which is acceptable.

As seen, a wireless link is 10 times worse than an unshielded telephone cable. This would mean that almost each telegram must be repeated. The BER of wireless systems can be improved to be around 10^{-5} through modulation techniques. But according to the example above, this means that each 100th telegram must be repeated. But this excludes a wireless solution for some applications, especially applications with very high requirements on latency and reliablity.

Bit error rate	10^{-4}	10^{-5}	10^{-9}
Corrupted telegrams	1/10	1/100	1/1000000
Repetition of corrupted telegrams	1s	10s	24h

Table 4: Influence of BER on telegram (128 Byte / 1024 Bit) repetition, send each 100 ms .

4.2 CLASSES OF INDUSTRIAL APPLICATIONS

Due to the general conditions in industrial applications, six classes of applications have been identified with tight requirements on the conditions described above. Depending on the application, the security and reliability as latency time of transmission differs from not very important to absolutely necessary.

Category	NAMUR	SP100	Application	Description
Safety	A	0	Emergency action	Always critical
Control	B	1	Closed loop regulatory control	Often critical
		2	Closed loop supervisory control	Usually noncritical
		3	Open loop control	Human in the loop
Monitoring	C	4	Alerting	Short-term operational consequence (e.g., event-based maintenance)
		5	Logging and down-loading/uploading	No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)

TIME

Table 5: Application classes in industrial automation

Today, the focus for industrial wireless utilization is concentrated in classes 3 to 5, which is mainly logging and parameterization of devices, and alerting and open loop control applications. Those applications are not time critical. So if a message gets lost, there is enough time to repeat the message or reroute it through a mesh network.

For the other classes, 0 to 2, special measures must be taken to complete the timing requirements and avoid decreasing the availability of the application. For example, a safety system detects a dangerous situation every time the signal is interrupted. Since the wireless communication can be interrupted randomly, each interruption will cause a shutdown. This is very safe, but not desired since downtime will increase.

4.3 SPECIAL CONDITIONS FOR USING WIRELESS TECHNOLOGY

Apart from the general conditions for wireless networks used in industrial automation, different detail conditions apply for factory and process automation areas.

4.3.1 FACTORY AUTOMATION

Factory automation is characterized by machine and assembly tools that perform milling, cutting, screwing, pressing, and welding of bulk goods. All of these are done with fast movements of slides, tools, or robot arms having a limited radius.

Eighty percent (80 %) of all sensors used in factory automation are simple proximity switches. The switching condition can be coded in one bit, and then transmitted over a small range since the movements are limited. Usually, the range is less than 10 m, which moves the importance of range in a wireless communication to second priority.

Due to the fast movements within the application, the switching condition must be transmitted quickly; 10 ms are a common time frame. ZigBee could almost meet this requirement. The latency times of ZigBee is 10 ms, but without repetition. For fast movements of motion control on numerical control (NC) machines, 1 ms is required. For this, a special solution must be developed. Also, the fast data transmission needs high power, making it difficult to develop battery-powered sensors.

Also, the movements create a constantly changing environment, which might increase the loss of data packages. To alleviate this problem, senders and receivers must be chosen to level this out.

Another application used in factory automation are guideless transport vehicles controlled wirelessly. Latency times are not as extreme, but there can be more data on position and speed, and the range must be much higher since the vehicles cover distance.

4.3.2 PROCESS AUTOMATION

Process automation is mainly characterized by heating, cooling, stirring, mixing, batching, and pumping substances. There are seldom any moving parts; tanks, pumps, solenoids, and pipelines are immobile.

Mostly, analog values must be retrieved as level, temperature and pressure, which can be represented by 2 – 4 bytes. Since these values change slowly, 100 ms to 1 s can be considered realtime for these applications. This can easily be met with wireless technologies. Repetition of the signal and hopping through a mesh network can be processed in a given timeframe. But the distances of process automation facilities are much larger, so range is a very important factor. The range which can be required in PA facilities can be from 100 m to a few km. A 900 MHz system can bridge up to 1 km, a 2.4 GHz system up to 300 m in best conditions.

To cover a larger range, either multiple access points must be installed or a mesh network can be utilized.

The environment in facilities rarely changes; for the most part it is static. By carefully choosing the sender and receiver positions, as well as utilizing mesh networks, this can be controlled in certain limits.

4.3.3 CONCLUSION

- Industrial applications require reliable, safe, and secure communication.
- Industrial communication serves different classes of applications.
- Some of these classes can be realized easily with wireless.
- In addition to the general requirements, factory automation and process automation require different properties in terms of communication speed, distance, data rate, information size, latency, etc. Specialized systems for both main fields may exist.

TABLES

Table 1:	Path loss exponent for different environments	7
Table 2:	Encryption concept WEP	24
Table 3:	Bit error rates for industrial automation	38
Table 4:	Influence of BER on telegram repetition	39
Table 5:	Application classes in industrial automation	39

GRAPHICS

Figure 1:	Electromagnetic spectrum	4
Figure 2:	Light refraction on a prism	4
Figure 3:	Inverse square law	5
Figure 4:	Theoretical free space propagation	6
Figure 5:	Practical propagation	7
Figure 6:	Diffusion, reflection, bending, and penetration of obstacles	9
Figure 7:	Positively superimposed wave	9
Figure 8:	Negatively superimposed wave	9
Figure 9:	Interference of two circular waves	10
Figure 10:	Receipt of the original signal (reflections, bendings and diffusions)	10

5 TABLES, FIGURES AND SOURCES

Figure 11: Fresnel zone and possible disruptions 11
Figure 12: Amplitude modulation 13
Figure 13: Frequency hopping spread spectrum 14
Figure 14: Direct sequence spread spectrum 15
Figure 15: Radiation pattern of undisturbed dipole antenna 17
Figure 16: Radiation pattern of dipole 17
Figure 17: Reception quality depending on radiation pattern and relative position of radios 18
Figure 18: Radiation pattern of omni-directional and directional antennas 18
Figure 19: Power and energy density of different battery types 22
Figure 20: Shift cypher through shifting of 3 characters 23
Figure 21: AES encryption process 25
Figure 22: Result of using ECB mode or non-ECB modes for encryption 26
Figure 23: ISM bands 27
Figure 24: Channel designation in 2.4GHz band according to IEEE 802.1 29
Figure 25: Channel designation in 2.4GHz band according to IEEE 802.15.1 29
Figure 26: Channel designation in 2.4GHz band according to IEEE 802.15.4 30
Figure 27: Standards for WPAN, WLAN, WMAN, and WWAN 31
Figure 28: Wireless standards and their properties 31
Figure 29: Overlapping of time, frequency and location 32
Figure 30: Star network 34
Figure 31: Mesh network 35
Figure 32: Star-mesh network 36

SOURCES

Following sources have been used to assemble this brochure:

http://de.wikipedia.org/wiki/Elektromagnetisches_Spektrum

Presentation: Vergleich des IEEE802.15.4 Standards in verschiedenen Frequenzbändern, Dipl.-Ing. Udo Walter, ZMD AG, Wireless Technology Congress, October 2005 in Mannheim

Das Mobilfunknetz, Vincent Langenfeld, 3. Dezember 2007

Artikel: Grundlagen der drahtlosen Übertragung, Dragan Popovic, Fachhochschule Wedel –Informatikseminar WS2004, Prof. Dr. Sebastian Iwanowski Wedel –Informatik-seminar WS2004, Prof. Dr. Sebastian Iwanowski

Article: Ask the experts: Environmental effects on wireless, by John Welch, Apprion, February 22nd 2011

http://en.wikipedia.org/wiki/Fresnel_zone
http://de.wikipedia.org/wiki/Interferenz_(Physik)
http://de.wikipedia.org/wiki/Amplitudenmodulation
http://de.wikipedia.org/wiki/FHSS

http://de.wikipedia.org/wiki/DSSS
http://de.wikipedia.org/wiki/Antennentechnik
http://de.wikipedia.org/wiki/Antennendiagramm
http://de.wikipedia.org/wiki/Energy_harvesting
http://de.wikipedia.org/wiki/Batterie_(Elektrotechnik)
http://en.wikipedia.org/wiki/Rechargeable_battery
http://de.wikipedia.org/wiki/Kryptographie
http://de.wikipedia.org/wiki/Data_Encryption_Standard
http://de.wikipedia.org/wiki/Wired_Equivalent_Privacy
http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
http://de.wikipedia.org/wiki/WPA2
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Electronic_codebook_.28ECB.29
http://de.wikipedia.org/wiki/Frequenzband
http://de.wikipedia.org/wiki/ISM-Band
http://de.wikipedia.org/wiki/WPAN
http://de.wikipedia.org/wiki/WLAN
http://de.wikipedia.org/wiki/IEEE_802.11
http://de.wikipedia.org/wiki/IEEE_802.15.1
http://de.wikipedia.org/wiki/Bluetooth
http://de.wikipedia.org/wiki/IEEE_802.15.4
http://de.wikipedia.org/wiki/ZigBee

Koexistenz von Funksystemen in der Automatisierungstechnik, Erläuterungen zum Zuverlässigen Parallelbetrieb von Funklösungen, ZVEI – Zentralverband Elektrotechnik und Elektroindustrie e.V., Fachverband Automation, Lyoner Straße 9, 60528 Frankfurt am Main, Deutschland

http://de.wikipedia.org/wiki/Topologie_(Rechnernetz)

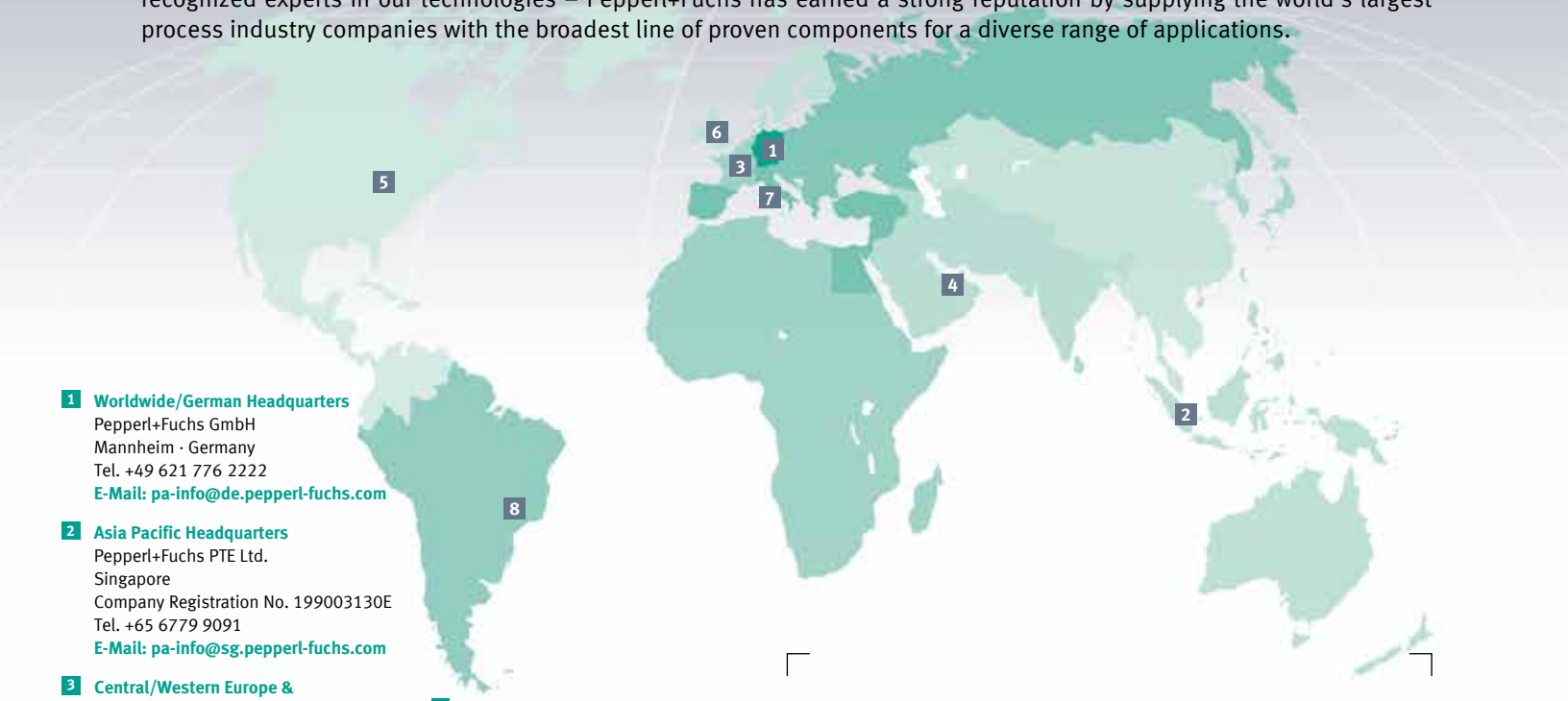
Presentation: Drahtlose Erfassung von Sensoren und Aktoren in der Prozessindustrie, Dipl.-Ing. Frank Hakemeyer, Phoenix Contact GmbH, Wireless Technology Congress, October 2005 in Mannheim

http://en.wikipedia.org/wiki/Bit_error_rate

Presentation: IEEE 802.15.4 / ZigBee und Funktionale Sicherheit in der Automation, Heiko Adamczyk, Dr. Lutz Rauchhaupt, Institut für Automation und Kommunikation e.V. Magdeburg, Wireless Technology Congress, October 2005 in Mannheim

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

For over a half century, Pepperl+Fuchs has provided new concepts for the world of process automation. Our company sets standards in quality and innovative technology. We develop, produce and distribute electronic interface modules, Human-Machine Interfaces and hazardous location protection equipment on a global scale, meeting the most demanding needs of industry. Our worldwide presence, combined with flexible operating systems in our production and service organizations, enable us to offer complete individual solutions – wherever and whenever you need us. We are the recognized experts in our technologies – Pepperl+Fuchs has earned a strong reputation by supplying the world's largest process industry companies with the broadest line of proven components for a diverse range of applications.



1 Worldwide/German Headquarters
Pepperl+Fuchs GmbH
Mannheim · Germany
Tel. +49 621 776 2222
E-Mail: pa-info@de.pepperl-fuchs.com

2 Asia Pacific Headquarters
Pepperl+Fuchs PTE Ltd.
Singapore
Company Registration No. 199003130E
Tel. +65 6779 9091
E-Mail: pa-info@sg.pepperl-fuchs.com

3 Central/Western Europe & Africa Headquarters
Pepperl+Fuchs N.V.
Schoten/Antwerp · Belgium
Tel. +32 3 6442500
E-Mail: pa-info@be.pepperl-fuchs.com

4 Middle East Headquarters
Pepperl+Fuchs M.E (FZE)
Dubai · UAE
Tel. +971 4 883 8378
E-Mail: pa-info@ae.pepperl-fuchs.com

5 North/Central America Headquarters
Pepperl+Fuchs Inc.
Twinsburg · Ohio · USA
Tel. +1 330 486 0002
E-Mail: pa-info@us.pepperl-fuchs.com

6 Northern Europe Headquarters
Pepperl+Fuchs GB Ltd.
Oldham · England
Tel. +44 161 6336431
E-Mail: pa-info@gb.pepperl-fuchs.com

7 Southern/Eastern Europe Headquarters
Pepperl+Fuchs Elcon srl
Sulbiate · Italy
Tel. +39 039 62921
E-Mail: pa-info@it.pepperl-fuchs.com

8 South America Headquarters
Pepperl+Fuchs Ltda.
São Bernado do Campo · SP · Brazil
Tel. +55 11 4341 8448
E-Mail: pa-info@br.pepperl-fuchs.com

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS